



FortiOS™
CLI Reference for FortiOS 5.0



FortiOS™ CLI Reference for FortiOS 5.0

August 31, 2016

01-509-99686-20160831

Copyright© 2016 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

| | |
|----------------------------|---|
| Technical Documentation | docs.fortinet.com |
| Knowledge Base | kb.fortinet.com |
| Customer Service & Support | support.fortinet.com |
| Training Services | training.fortinet.com |
| FortiGuard | fortiguard.com |
| Document Feedback | techdocs@fortinet.com |

Contents

| | |
|---|-----------|
| Introduction..... | 19 |
| How this guide is organized..... | 19 |
| Availability of commands and options..... | 19 |
| Managing Firmware with the FortiGate BIOS..... | 20 |
| Accessing the BIOS..... | 20 |
| Navigating the menu..... | 20 |
| Loading firmware..... | 21 |
| Configuring TFTP parameters..... | 21 |
| Initiating TFTP firmware transfer..... | 22 |
| Booting the backup firmware..... | 22 |
| What's new..... | 23 |
| alertemail..... | 55 |
| setting..... | 56 |
| antivirus..... | 60 |
| heuristic..... | 61 |
| mms-checksum..... | 62 |
| notification..... | 63 |
| profile..... | 64 |
| config {http https ftp ftps imap imaps mapi pop3 pop3s smb smtp | |
| smtps nntp im}..... | 65 |
| config nac-quar..... | 66 |
| quarantine..... | 67 |
| service..... | 70 |
| settings..... | 71 |
| application..... | 72 |
| custom..... | 73 |
| list..... | 74 |
| name..... | 78 |
| client-reputation..... | 79 |
| profile..... | 80 |
| dlp..... | 82 |
| filepattern..... | 83 |
| fp-doc-source..... | 85 |
| fp-sensitivity..... | 87 |
| sensor..... | 88 |
| settings..... | 90 |

| | |
|--|-----------|
| endpoint-control | 91 |
| forticlient-registration-sync | 92 |
| profile | 93 |
| settings | 98 |
| firewall | 99 |
| address, address6 | 100 |
| addrgrp, addrgrp6 | 103 |
| auth-portal | 104 |
| carrier-endpoint-bwl | 105 |
| carrier-endpoint-ip-filter | 107 |
| central-nat | 108 |
| deep-inspection-options | 109 |
| config ftps | 110 |
| config https | 111 |
| config imaps | 111 |
| config pop3s | 112 |
| config smtps | 112 |
| config ssl | 113 |
| config ssl-server | 113 |
| dnstranslation | 115 |
| DoS-policy, DoS-policy6 | 116 |
| gtp | 118 |
| identity-based-route | 134 |
| interface-policy | 135 |
| interface-policy6 | 137 |
| ipmacbinding setting | 139 |
| ipmacbinding table | 140 |
| ippool, ippool6 | 141 |
| ip-translation | 143 |
| ipv6-eh-filter | 144 |
| ldb-monitor | 145 |
| local-in-policy, local-in-policy6 | 147 |
| mms-profile | 148 |
| config dupe {mm1 mm4} | 155 |
| config flood {mm1 mm4} | 157 |
| config log | 158 |
| config notification {alert-dupe-1 alert-flood-1 mm1 mm3 mm4 mm7} | 158 |
| config notif-msisdn | 162 |
| multicast-address | 163 |
| multicast-policy | 165 |
| policy, policy6 | 167 |
| config identity-based-policy | 184 |

| | |
|--------------------------------|------------|
| policy46, policy64 | 186 |
| profile-group | 188 |
| profile-protocol-options | 190 |
| config http | 192 |
| config ftp | 193 |
| config dns | 194 |
| config imap | 194 |
| config mapi | 195 |
| config pop3 | 195 |
| config smtp | 196 |
| config nntp | 197 |
| config im | 198 |
| config mail-signature | 198 |
| schedule onetime | 199 |
| schedule recurring | 200 |
| schedule group | 201 |
| service category | 202 |
| service custom | 203 |
| service group | 207 |
| shaper per-ip-shaper | 208 |
| shaper traffic-shaper | 210 |
| sniffer | 211 |
| sniff-interface-policy | 214 |
| sniff-interface-policy6 | 217 |
| ssl setting | 220 |
| ttl-policy | 221 |
| vip | 222 |
| vip46 | 242 |
| vip6 | 244 |
| vip64 | 246 |
| vipgrp | 248 |
| vipgrp46 | 249 |
| vipgrp64 | 250 |
| ftp-proxy | 251 |
| explicit | 252 |
| gui | 253 |
| console | 254 |
| icap | 255 |
| profile | 256 |
| server | 257 |

| | |
|--|------------|
| imp2p | 258 |
| aim-user | 259 |
| icq-user | 260 |
| msn-user | 261 |
| old-version | 262 |
| policy | 263 |
| yahoo-user | 264 |
| ips | 265 |
| custom | 266 |
| decoder | 267 |
| global | 268 |
| rule | 270 |
| sensor | 271 |
| setting | 276 |
| log | 277 |
| custom-field | 278 |
| {disk fortianalyzer fortianalyzer2 fortianalyzer3 memory syslogd syslogd2 syslogd3 webtrends fortiguard} filter | 279 |
| disk setting | 283 |
| eventfilter | 287 |
| {fortianalyzer syslogd} override-filter | 288 |
| fortianalyzer override-setting | 289 |
| {fortianalyzer fortianalyzer2 fortianalyzer3} setting | 290 |
| fortiguard setting | 293 |
| gui-display | 294 |
| memory setting | 295 |
| memory global-setting | 296 |
| setting | 297 |
| syslogd override-setting | 299 |
| {syslogd syslogd2 syslogd3} setting | 301 |
| webtrends setting | 303 |
| netscan | 304 |
| assets | 305 |
| settings | 307 |
| pbx | 309 |
| dialplan | 310 |
| did | 312 |
| extension | 313 |
| global | 315 |
| ringgrp | 317 |

| | |
|---|------------|
| voice-menu | 318 |
| sip-trunk..... | 319 |
| report | 321 |
| chart..... | 322 |
| dataset | 327 |
| layout | 328 |
| style..... | 333 |
| summary | 337 |
| theme | 338 |
| router | 341 |
| access-list, access-list6 | 342 |
| aspath-list | 344 |
| auth-path | 345 |
| bfd..... | 346 |
| bgp..... | 347 |
| config router bgp | 351 |
| config admin-distance | 354 |
| config aggregate-address, config aggregate-address6 | 355 |
| config neighbor | 356 |
| config network, config network6 | 365 |
| config redistribute, config redistribute6 | 366 |
| community-list | 367 |
| gwdetect | 369 |
| isis..... | 370 |
| config isis-interface..... | 374 |
| config isis-net..... | 375 |
| config redistribute {bgp connected ospf rip static} | 375 |
| config summary-address | 376 |
| key-chain | 377 |
| multicast | 379 |
| Sparse mode..... | 379 |
| Dense mode..... | 380 |
| config router multicast | 382 |
| config interface | 383 |
| config pim-sm-global..... | 386 |
| multicast6 | 391 |
| multicast-flow | 392 |
| ospf..... | 393 |
| config router ospf..... | 396 |
| config area | 398 |
| config distribute-list | 403 |
| config neighbor | 404 |

| | |
|--|------------|
| config network | 405 |
| config ospf-interface | 405 |
| config redistribute | 409 |
| config summary-address | 410 |
| ospf6 | 411 |
| policy, policy6 | 417 |
| prefix-list, prefix-list6 | 421 |
| rip | 423 |
| config router rip | 424 |
| config distance | 426 |
| config distribute-list | 426 |
| config interface | 427 |
| config neighbor | 429 |
| config network | 430 |
| config offset-list | 430 |
| config redistribute | 431 |
| ripng | 432 |
| config distance | 434 |
| route-map | 438 |
| Using route maps with BGP | 440 |
| setting | 445 |
| static | 446 |
| static6 | 448 |
| spamfilter | 449 |
| bwl | 450 |
| bword | 453 |
| dnsbl | 455 |
| fortishield | 457 |
| iptrust | 459 |
| mheader | 460 |
| options | 462 |
| profile | 463 |
| config {imap imaps mapi pop3 pop3s smtp smtps} | 465 |
| config {gmail msn-hotmail yahoo-mail} | 466 |
| switch-controller | 467 |
| managed-switch | 468 |
| vlan | 469 |
| system | 470 |
| 3g-modem custom | 472 |
| accprofile | 473 |
| admin | 476 |
| amc | 485 |

| | |
|------------------------------|-----|
| arp-table | 486 |
| auto-install | 487 |
| autoupdate push-update | 488 |
| autoupdate schedule | 489 |
| autoupdate tunneling | 490 |
| aux | 491 |
| bug-report..... | 492 |
| bypass | 493 |
| central-management..... | 494 |
| console | 496 |
| ddns | 497 |
| dedicated-mgmt | 499 |
| dhcp reserved-address..... | 500 |
| dhcp server | 501 |
| dhcp6 server | 506 |
| dns | 508 |
| dns-database..... | 509 |
| dns-server..... | 512 |
| elbc | 513 |
| email-server | 514 |
| fips-cc | 515 |
| fortiguard | 516 |
| fortisandbox..... | 520 |
| geoip-override..... | 521 |
| gi-gk..... | 522 |
| global | 523 |
| gre-tunnel..... | 542 |
| ha | 543 |
| interface | 555 |
| ipip-tunnel | 583 |
| ips-urlfilter-dns..... | 584 |
| ipv6-neighbor-cache..... | 585 |
| ipv6-tunnel | 586 |
| mac-address-table | 587 |
| modem..... | 588 |
| monitors | 592 |
| nat64 | 594 |
| network-visibility | 595 |
| np6 | 596 |
| npu | 600 |

| | |
|---|-----|
| ntp..... | 601 |
| object-tag | 602 |
| password-policy | 603 |
| physical-switch | 604 |
| port-pair | 605 |
| probe-response | 606 |
| proxy-arp | 607 |
| pstn | 608 |
| replacemsg admin | 610 |
| replacemsg alertmail..... | 611 |
| replacemsg auth | 613 |
| replacemsg device-detection-portal..... | 617 |
| replacemsg ec | 618 |
| replacemsg fortiguard-wf | 620 |
| replacemsg ftp..... | 622 |
| replacemsg http..... | 624 |
| replacemsg im | 627 |
| replacemsg mail..... | 629 |
| replacemsg mm1 | 632 |
| replacemsg mm3 | 635 |
| replacemsg mm4 | 637 |
| replacemsg mm7 | 639 |
| replacemsg-group | 642 |
| replacemsg-group | 644 |
| replacemsg-image | 647 |
| replacemsg nac-quar..... | 648 |
| replacemsg nntp | 650 |
| replacemsg spam | 652 |
| replacemsg sslvpn..... | 655 |
| replacemsg traffic-quota | 656 |
| replacemsg utm..... | 657 |
| replacemsg webproxy | 659 |
| resource-limits | 660 |
| server-probe | 662 |
| session-helper | 663 |
| session-sync..... | 665 |
| session-ttl | 668 |
| settings | 670 |
| sit-tunnel | 677 |
| sflow..... | 678 |

| | |
|--|------------|
| sms-server | 679 |
| snmp community | 680 |
| snmp sysinfo | 684 |
| snmp user | 686 |
| sp | 689 |
| storage | 691 |
| stp | 692 |
| switch-interface | 693 |
| tos-based-priority | 695 |
| vdom-dns | 696 |
| vdom-link | 697 |
| vdom-property | 698 |
| vdom-radius-server | 701 |
| vdom-sflow | 702 |
| virtual-switch | 703 |
| wccp | 704 |
| zone | 707 |
| user | 708 |
| Configuring users for authentication | 709 |
| Configuring users for password authentication | 709 |
| Configuring peers for certificate authentication | 709 |
| ban | 710 |
| device | 713 |
| device-access-list | 714 |
| device-category | 715 |
| device-group | 716 |
| fortitoken | 717 |
| fsso | 718 |
| fsso-polling | 720 |
| group | 722 |
| ldap | 726 |
| local | 729 |
| password-policy | 731 |
| peer | 732 |
| peergrp | 734 |
| radius | 735 |
| setting | 740 |
| tacacs+ | 742 |
| voip | 743 |
| profile | 744 |

| | |
|--|------------|
| config sip | 746 |
| config sccp | 755 |
| vpn | 756 |
| certificate ca | 757 |
| certificate crt | 758 |
| certificate local..... | 760 |
| certificate ocsp-server | 762 |
| certificate remote..... | 763 |
| certificate setting | 764 |
| ipsec concentrator..... | 765 |
| ipsec forticlient..... | 766 |
| ipsec manualkey | 767 |
| ipsec manualkey-interface..... | 770 |
| ipsec phase1 | 773 |
| ipsec phase1-interface | 782 |
| ipsec phase2..... | 796 |
| ipsec phase2-interface | 803 |
| l2tp | 812 |
| pptp | 814 |
| ssl settings..... | 816 |
| ssl web host-check-software..... | 820 |
| ssl web portal..... | 822 |
| ssl web realm..... | 831 |
| ssl web user | 832 |
| ssl web virtual-desktop-app-list | 834 |
| wanopt..... | 835 |
| auth-group | 836 |
| peer..... | 837 |
| profile | 838 |
| settings | 842 |
| ssl-server | 843 |
| storage..... | 846 |
| webcache | 847 |
| webfilter..... | 850 |
| content..... | 851 |
| content-header | 853 |
| fortiguard | 854 |
| ftgd-local-cat | 856 |
| ftgd-local-rating | 857 |
| ftgd-warning | 858 |

| | |
|----------------------------------|------------|
| ips-urlfilter-cache-setting..... | 860 |
| ips-urlfilter-setting..... | 861 |
| override..... | 862 |
| override-user..... | 863 |
| profile..... | 865 |
| config ftgd-wf..... | 869 |
| config override..... | 871 |
| config quota..... | 871 |
| config web..... | 872 |
| search-engine..... | 873 |
| urlfilter..... | 874 |
| web-proxy..... | 876 |
| explicit..... | 877 |
| forward-server..... | 881 |
| forward-server-group..... | 882 |
| global..... | 883 |
| url-match..... | 885 |
| wireless-controller..... | 886 |
| ap-status..... | 887 |
| global..... | 888 |
| setting..... | 889 |
| timers..... | 890 |
| vap..... | 891 |
| wids-profile..... | 895 |
| wtp..... | 897 |
| wtp-profile..... | 901 |
| execute..... | 906 |
| backup..... | 907 |
| batch..... | 910 |
| bypass-mode..... | 911 |
| carrier-license..... | 912 |
| central-mgmt..... | 913 |
| cfg reload..... | 914 |
| cfg save..... | 915 |
| clear system arp table..... | 916 |
| cli check-template-status..... | 917 |
| cli status-msg-only..... | 918 |
| client-reputation..... | 919 |
| date..... | 920 |
| disk..... | 921 |

| | |
|---|-----|
| disk raid | 922 |
| dhcp lease-clear | 923 |
| dhcp lease-list | 924 |
| disconnect-admin-session | 925 |
| enter | 926 |
| erase-disk | 927 |
| factoryreset | 928 |
| factoryreset2 | 929 |
| formatlogdisk | 930 |
| forticarrier-license | 931 |
| forticlient | 932 |
| fortiguard-log | 933 |
| fortisandbox test-connectivity | 934 |
| fortitoken | 935 |
| fortitoken-mobile | 936 |
| fsso refresh | 937 |
| ha disconnect | 938 |
| ha ignore-hardware-revision | 939 |
| ha manage | 940 |
| ha synchronize | 941 |
| interface dhcpclient-renew | 942 |
| interface pppoe-reconnect | 943 |
| log client-reputation-report | 944 |
| log convert-oldlogs | 945 |
| log delete-all | 946 |
| log delete-oldlogs | 947 |
| log display | 948 |
| log filter | 949 |
| log fortianalyzer test-connectivity | 950 |
| log list | 951 |
| log rebuild-sqldb | 952 |
| log recreate-sqldb | 953 |
| log-report reset | 954 |
| log roll | 955 |
| log upload-progress | 956 |
| modem dial | 957 |
| modem hangup | 958 |
| modem trigger | 959 |
| mroutel clear | 960 |
| netscan | 961 |

| | |
|---------------------------------------|------|
| pbx | 962 |
| ping | 964 |
| ping-options, ping6-options | 965 |
| ping6 | 967 |
| policy-packet-capture delete-all..... | 968 |
| reboot | 969 |
| report | 970 |
| report-config reset | 971 |
| restore..... | 972 |
| revision..... | 976 |
| router clear bfd session | 977 |
| router clear bgp | 978 |
| router clear ospf process..... | 979 |
| router restart | 980 |
| send-fds-statistics | 981 |
| set system session filter | 982 |
| set-next-reboot..... | 984 |
| sfp-mode-sgmii | 985 |
| shutdown | 986 |
| ssh | 987 |
| sync-session | 988 |
| tac report | 989 |
| telnet | 990 |
| time | 991 |
| traceroute..... | 992 |
| tracert6..... | 993 |
| update-ase..... | 994 |
| update-av..... | 995 |
| update-geo-ip | 996 |
| update-ips..... | 997 |
| update-now..... | 998 |
| update-src-vis..... | 999 |
| upd-vd-license..... | 1000 |
| upload | 1001 |
| usb-device | 1002 |
| usb-disk | 1003 |
| vpn certificate ca | 1004 |
| vpn certificate crl | 1005 |
| vpn certificate local..... | 1006 |
| vpn certificate remote..... | 1009 |

| | |
|--|-------------|
| vpn ipsec tunnel down..... | 1010 |
| vpn ipsec tunnel up | 1011 |
| vpn sslvpn del-all..... | 1012 |
| vpn sslvpn del-tunnel..... | 1013 |
| vpn sslvpn del-web..... | 1014 |
| vpn sslvpn list | 1015 |
| webfilter quota-reset..... | 1016 |
| wireless-controller delete-wtp-image | 1017 |
| wireless-controller list-wtp-image | 1018 |
| wireless-controller reset-wtp | 1019 |
| wireless-controller restart-acd | 1020 |
| wireless-controller restart-wtpd..... | 1021 |
| wireless-controller upload-wtp-image | 1022 |
| get..... | 1023 |
| endpoint-control app-detect | 1024 |
| firewall dnstranslation | 1026 |
| firewall iprope appctrl | 1027 |
| firewall iprope list..... | 1028 |
| firewall proute, proute6..... | 1029 |
| firewall service custom | 1030 |
| firewall shaper..... | 1031 |
| grep..... | 1032 |
| gui console status..... | 1033 |
| gui topology status | 1034 |
| hardware cpu..... | 1035 |
| hardware memory..... | 1037 |
| hardware nic | 1038 |
| hardware npu..... | 1039 |
| hardware status | 1042 |
| ips decoder status | 1043 |
| ips rule status..... | 1044 |
| ips session | 1045 |
| ipsec tunnel..... | 1046 |
| ips view-map | 1047 |
| mgmt-data status | 1048 |
| netscan settings..... | 1049 |
| pbx branch-office | 1050 |
| pbx dialplan | 1051 |
| pbx did..... | 1052 |
| pbx extension | 1053 |

| | |
|--|------|
| pbx ftgd-voice-pkg | 1054 |
| pbx global | 1055 |
| pbx ringgrp | 1056 |
| pbx sip-trunk..... | 1057 |
| pbx voice-menu | 1058 |
| report database schema..... | 1059 |
| router info bfd neighbor | 1060 |
| router info bgp | 1061 |
| router info gwdetect..... | 1064 |
| router info isis | 1065 |
| router info kernel..... | 1066 |
| router info multicast | 1067 |
| router info ospf | 1069 |
| router info protocols | 1071 |
| router info rip | 1072 |
| router info routing-table | 1073 |
| router info vrrp | 1074 |
| router info6 bgp | 1075 |
| router info6 interface..... | 1076 |
| router info6 kernel..... | 1077 |
| router info6 ospf | 1078 |
| router info6 protocols | 1079 |
| router info6 rip | 1080 |
| router info6 routing-table | 1081 |
| system admin list | 1082 |
| system admin status..... | 1083 |
| system arp | 1084 |
| system auto-update..... | 1085 |
| system central-management | 1086 |
| system checksum | 1087 |
| system cmdb status | 1088 |
| system fortianalyzer-connectivity | 1089 |
| system fortiguard-log-service status | 1090 |
| system fortiguard-service status | 1091 |
| system ha-nonsync-csum | 1092 |
| system ha status..... | 1093 |
| system info admin ssh | 1096 |
| system info admin status..... | 1097 |
| system interface physical | 1098 |
| system mgmt-csum | 1099 |

| | |
|---|-------------|
| system performance firewall..... | 1100 |
| system performance status | 1101 |
| system performance top..... | 1102 |
| system session list..... | 1103 |
| system session status | 1104 |
| system session-helper-info list | 1105 |
| system session-info | 1106 |
| system source-ip | 1107 |
| system startup-error-log..... | 1108 |
| system status..... | 1109 |
| test | 1110 |
| user adgrp..... | 1112 |
| vpn ike gateway..... | 1113 |
| vpn ipsec tunnel details | 1114 |
| vpn ipsec tunnel name..... | 1115 |
| vpn ipsec stats crypto | 1116 |
| vpn ipsec stats tunnel..... | 1117 |
| vpn ssl monitor | 1118 |
| vpn status l2tp | 1119 |
| vpn status pptp..... | 1120 |
| vpn status ssl..... | 1121 |
| webfilter ftgd-statistics | 1122 |
| webfilter status | 1124 |
| wireless-controller rf-analysis | 1125 |
| wireless-controller scan..... | 1126 |
| wireless-controller status..... | 1127 |
| wireless-controller vap-status | 1128 |
| wireless-controller wlchanlistlic | 1129 |
| wireless-controller wtp-status | 1132 |
| tree..... | 1134 |

Introduction

This document describes FortiOS™ 5.0 CLI commands used to configure and manage a FortiGate unit from the command line interface (CLI).

How this guide is organized

Most of the chapters in this document describe the commands for each configuration branch of the FortiOS™ CLI. The command branches and commands are in alphabetical order.

This document also contains the following sections:

[Managing Firmware with the FortiGate BIOS](#) describes how to change firmware at the console during FortiGate unit boot-up.

[What's new](#) describes changes to the 5.0 CLI.

config chapters describe the config commands.

[execute](#) describes execute commands.

[get](#) describes get commands.

[tree](#) describes the tree command.

Availability of commands and options

Some FortiOS™ CLI commands and options are not available on all FortiGate units. The CLI displays an error message if you attempt to enter a command or option that is not available. You can use the question mark '?' to verify the commands and options that are available.

Commands and options may not be available for the following reasons:

- **FortiGate model.** All commands are not available on all FortiGate models. For example, low end FortiGate models do not support the `aggregate interface type` option of the `config system interface` command.
- **Hardware configuration.** For example, some AMC module commands are only available when an AMC module is installed.
- **FortiOS Carrier, FortiGate Voice, FortiWiFi etc.** Commands for extended functionality are not available on all FortiGate models. The CLI Reference includes commands only available for FortiWiFi units, FortiOS Carrier, and FortiGate Voice units

Managing Firmware with the FortiGate BIOS

FortiGate units are shipped with firmware installed. Usually firmware upgrades are performed through the web-based manager or by using the CLI `execute restore` command. From the console, you can also interrupt the FortiGate unit's boot-up process to load firmware using the BIOS firmware that is a permanent part of the unit.

Using the BIOS, you can:

- view system information
- format the boot device
- load firmware and reboot (see [“Loading firmware” on page 21](#))
- reboot the FortiGate unit from the backup firmware, which then becomes the default firmware (see [“Booting the backup firmware” on page 22](#))

Accessing the BIOS

The BIOS menu is available only through direct connection to the FortiGate unit's Console port. During boot-up, “Press any key” appears briefly. If you press any keyboard key at this time, boot-up is suspended and the BIOS menu appears. If you are too late, the boot-up process continues as usual.

Navigating the menu

The main BIOS menu looks like this:

```
[C]: Configure TFTP parameters
[R]: Review TFTP parameters
[T]: Initiate TFTP firmware transfer
[F]: Format boot device
[Q]: Quit menu and continue to boot
[I]: System Information
[B]: Boot with backup firmware and set as default
[Q]: Quit menu and continue to boot
[H]: Display this list of options
```

Enter C,R,T,F,I,B,Q, or H:

Typing the bracketed letter selects the option. Input is case-sensitive. Most options present a submenu. An option value in square brackets at the end of the “Enter” line is the default value which you can enter simply by pressing Return. For example,

Enter image download port number [WAN1]:

In most menus, typing H re-lists the menu options and typing Q returns to the previous menu.

Loading firmware

The BIOS can download firmware from a TFTP server that is reachable from a FortiGate unit network interface. You need to know the IP address of the server and the name of the firmware file to download.

The downloaded firmware can be saved as either the default or backup firmware. It is also possible to boot the downloaded firmware without saving it.

Configuring TFTP parameters

Starting from the main BIOS menu

```
[C]: Configure TFTP parameters.
```

Selecting the VLAN (if VLANs are used)

```
[V]: Set local VLAN ID.
```

Choose port and whether to use DHCP

```
[P]: Set firmware download port.
```

The options listed depend on the FortiGate model. Choose the network interface through which the TFTP server can be reached. For example:

```
[0]: Any of port 1 - 7
```

```
[1]: WAN1
```

```
[2]: WAN2
```

```
Enter image download port number [WAN1]:
```

```
[D]: Set DHCP mode.
```

```
Please select DHCP setting
```

```
[1]: Enable DHCP
```

```
[2]: Disable DHCP
```

If there is a DHCP server on the network, select [1]. This simplifies configuration. Otherwise, select [2].

Non-DHCP steps

```
[I]: Set local IP address.
```

```
Enter local IP address [192.168.1.188]:
```

This is a temporary IP address for the FortiGate unit network interface. Use a unique address on the same subnet to which the network interface connects.

```
[S]: Set local subnet mask.
```

```
Enter local subnet mask [255.255.252.0]:
```

```
[G]: Set local gateway.
```

The local gateway IP address is needed if the TFTP server is on a different subnet than the one to which the FortiGate unit is connected.

TFTP and filename

```
[T]: Set remote TFTP server IP address.
```

```
Enter remote TFTP server IP address [192.168.1.145]:
```

```
[F]: Set firmware file name.
```

```
Enter firmware file name [image.out]:
```

Enter [Q] to return to the main menu.

Initiating TFTP firmware transfer

Starting from the main BIOS menu

```
[T]: Initiate TFTP firmware transfer.
    Please connect TFTP server to Ethernet port 'WAN1'.

    MAC: 00:09:0f:b5:55:28

    Connect to tftp server 192.168.1.145 ...

#####
Image Received.
Checking image... OK
Save as Default firmware/Backup firmware/Run image without
saving: [D/B/R]?
```

After you choose any option, the FortiGate unit reboots. If you choose [D] or [B], there is first a pause while the firmware is copied:

```
    Programming the boot device now.
    .....
    .....
```

Booting the backup firmware

You can reboot the FortiGate unit from the backup firmware, which then becomes the default firmware.

Starting from the main BIOS menu

```
[B]: Boot with backup firmware and set as default.
```

If the boot device contains backup firmware, the FortiGate unit reboots. Otherwise the unit responds:

```
    Failed to mount filesystem. . .
    Mount back up partition failed.
    Back up image open failed.
    Press 'Y' or 'y' to boot default image.
```

What's new

As the FortiOS Handbook has developed, the *FortiGate CLI Reference for FortiOS 5.0* has become a dictionary of FortiOS CLI commands defining each command and its options, ranges, defaults and dependencies. The CLI Reference now includes FortiOS Carrier commands and future versions will include FortiGate Voice commands.

The table below lists the CLI commands and options in FortiOS 5.0 that have changed since the last major release of FortiOS.

| Command | Change |
|--|---|
| <code>config antivirus profile</code> <code>edit <name_str></code> <code>set block-botnet-connections</code> <code>set extended-utm-log</code> <code>set ftgd-analytics</code> <code>set inspection-mode</code> <code>config http</code> <code>set avdb</code> <code>config mapi</code> <code>config smb</code> | New field. Enables blocking connections to known botnet servers. New field, Enables logging UTM events. New field. Enables FortiGuard Analytics. New field. Selects proxy or flow-based antivirus operation. Field removed. New subcommand. Configures MAPI protocol options. New subcommand. |
| <code>config antivirus quarantine</code> <code>set drop-infected pop3 mapi</code> <code>set store-infected imaps smtps pop3s https ftps</code> <code>set enable-auto-submit</code> <code>set sel-status</code> <code>set use-fpat</code> <code>set use-status</code> | New options. Support MAPI, POP3 protocols. New options. Support IMAPS, SMTPS, POP3S, HTTPS, FTPS protocols. Fields removed. Quarantine auto-submit feature removed. |
| <code>config antivirus quarfilepattern</code> | Command removed. FortiGuard quarantine auto-submit feature was removed. |
| <code>config antivirus settings</code> <code>set default-db flow-based</code> | Option removed. Use <code>inspection-mode</code> in <code>antivirus profile</code> . |
| <code>config application list</code> <code>edit <app_list_str></code> <code>set extended-utm-log</code> <code>set log</code> <code>set options</code> | New field, Enables logging UTM events. Field removed. Use traffic log application sensor name and application action fields instead. New field. Enables basic application signatures for DNS, HTTP, ICMP, SSL. |

| Command | Change |
|---|--|
| config entries | |
| edit <id_integer> | |
| set popularity | New field. Sets application popularity levels. |
| config client-reputation profile | New command. Configure client reputation tracking. |
| config dlp compound | Command removed. |
| config dlp filepattern | |
| edit <filepattern_list_int> | |
| config entries | |
| edit <filepattern_str> | |
| set action | Field removed. |
| set filter-by encrypted | New option. Catches files that could not be scanned because of encryption. |
| set active | Field removed. |
| config dlp rule | Command removed. See config dlp sensor . |
| config dlp sensor | |
| config filter | |
| edit <id> | |
| set proto http-get http-post | New field. Can separately detect HTTP-GET and HTTP-PUT protocols. |
| end | |
| config dlp settings | |
| set cache-mem-percent | New field. Sets amount of available memory used for caching. |
| config endpoint-control app-detect rule-list | Command removed. |
| config endpoint-control forticlient-registration-sync | New command. Configures peer FortiGate units for synchronization of Endpoint license registration. |
| config endpoint-control profile | |
| edit <profile_name> | |
| config forticlient-winmac-settings | New subcommands. Profile re-organized into separate sections for Windows/Mac, Android, and iOS. |
| config forticlient-android-settings | |
| config forticlient-ios-settings | |
| set forticlient-config-deployment | New field. Enables deployment of FortiClient settings from Endpoint Control profile. |
| set forticlient-log-upload | New field. Enables sending of FortiClient logs to a FortiAnalyzer unit via the FortiGate unit. |
| set forticlient-log-upload-server | New field. Sets FortiClient log upload server. |
| set forticlient-settings-lock | New fields. Locks FortiClient settings and sets password to unlock them. |
| set forticlient-settings-lock-passwd | |
| set forticlient-update-from-fmg | New field. Enables FortiClient update from FortiManager. |
| set forticlient-update-server | New field. Sets FortiClient update servers. |
| set forticlient-vpn-provisioning | New fields. Configure VPNs on FortiClient endpoints. |
| config forticlient-vpn-settings | |
| set forticlient-advanced-vpn | |
| set forticlient-advanced-vpn-buffer | |

| Command | Change |
|--|---|
| set type network-service | New option. |
| set users | New option. Specifies the users to whom this profile applies. |
| set user-groups | New option. Specifies the user groups to which this profile applies. |
| config service | New subcommand. Configures network-service address. |
| config endpoint-control settings | |
| set endpoint-profile | New field. Sets which endpoint profile to apply. |
| set forticlient-keepalive-interval | New field. Sets keepalive message interval. |
| set forticlient-reg-key-enforce | New fields. Enable enforcement of FortiClient registration. |
| set forticlient-reg-key | |
| set forticlient-reg-timeout | New field. Sets timeout of FortiClient registration. |
| set forticlient-sys-update-interval | New field. Sets update message interval. |
| set forticlient-temp-authorization-timeout | New field. Sets duration of temporary authorization. |
| set registration-password | New field. Sets a password for FortiClient updates. |
| config firewall addrgrp, addrgrp6 | An address group can be a member of another address group. |
| config firewall auth-portal | New command. Adds an external authentication portal. |
| config firewall deep-inspection-options | New command. Sets deep inspection options for secure protocols, such as HTTPS, FTPS, etc. |
| config firewall DoS-policy, DoS-policy6 | New command. Replaces config ips DoS. |
| config firewall gtp | |
| edit <name_str> | |
| set unknown-version-action | New field. Allow or deny traffic with GTP version > 1. |
| config firewall identity-based-route | New command. Configures identity-based routes. |
| config firewall ippool | |
| set arp-enable | New fields. Can limit ARP requests to one interface or disable them completely. |
| set arp-intf | |
| set block-size | New fields. Set block size and blocks/user for new port-block-allocation IP pool type. |
| set num-blocks-per-user | |
| set source-startip | New fields. Define the source IP range for fixed port range mapping. |
| set source-endip | |
| set type | Field added. Select type of mapping. |
| config firewall ippool6 | New command. Configures IPv6 IP pools. |
| config firewall ip-translation | New command. Configures IP address translation. |
| config firewall ipv6-eh-filter | New command. Configures IPv6 routing header packet filtering. |
| config firewall mms-profile | |
| set mm1 strict-file | Option strict-file is obsolete and was removed. |
| set mm7 strict-file | |

| Command | Change |
|--|--|
| <code>config firewall multicast-address</code> | New command. Configures multicast firewall addresses. |
| <code>config firewall multicast-policy</code> | |
| <code>edit <index_int></code> | |
| <code>set dstaddr</code> | This field now accepts multicast address names defined in <code>firewall multicast-address</code> . |
| <code>set srcaddr</code> | This field now accepts address names defined in <code>firewall address</code> , <code>address6</code> . |
| <code>set nat</code> | Field removed. Use <code>snat</code> . |
| <code>set snat</code> | New field. Enables substitution of outgoing interface IP address for the original source IP address. |
| <code>config firewall policy, policy6</code> | |
| <code>edit <policy_id></code> | The <code>nat</code> , <code>ippool</code> and <code>poolname</code> fields now also apply to <code>policy6</code> . |
| <code>set active-auth-method</code> | New field. Specifies active authentication method, which is used if <code>sso-auth-method</code> fails. |
| <code>set application-list</code> | This field is now also available in IPv6 policies. |
| <code>set auth-method</code> | Field removed. Use <code>sso-auth-method</code> and <code>active-auth-method</code> . |
| <code>set auth-portal</code> | New field. Enables use of external authentication portal defined in <code>firewall auth-portal</code> . |
| <code>set block-notification</code> | New field. Enables Fortinet Bar notification of blocked files. |
| <code>set capture-packet</code> | New field. Enables packet capture in policy. |
| <code>set client-reputation</code> | New field. Enables Client Reputation in policy. |
| <code>set device-detection-portal</code> | New field. Enables the Device Detection portal. |
| <code>set dstaddr-negate</code> | New field. Negates <code>dstaddr</code> selection. |
| <code>set dstintf</code> | Field now accepts multiple interface names. |
| <code>set dynamic-profile</code> | Fields removed. Dynamic profile is controlled in the interface. |
| <code>set dynamic-profile-group</code> | |
| <code>set dynamic-profile-access</code> | Field removed. RADIUS SSO replaces dynamic profile feature. |
| <code>set email-collection-portal</code> | New field. Enables email collection from new devices. |
| <code>set fall-through-unauthenticated</code> | New field. Enables unauthenticated user to skip authentication rules and possibly match another policy. |
| <code>set forticlient-compliance-devices</code> | New field. Select device types to which FortiClient enforcement applies. |
| <code>set deep-inspection-options</code> | New field. Applies a deep inspection options profile. |
| <code>set forticlient-compliance-enforcement-portal</code> | New field. Enables the FortiClient portal. |
| <code>set identity-based-route</code> | New field. Enables use of identity-based route defined in <code>firewall identity-based-route</code> . |
| <code>set identity-from</code> | New field. Selects whether identity comes from authenticated user or device. |

| Command | Change |
|--|---|
| config firewall policy , policy6 (continued) | |
| set ips-DoS-status | Fields removed. Use <code>config firewall DoS-policy</code> command. |
| set ips-DoS | |
| set ips-sensor | This field is now also available in IPv6 policies. |
| set logtraffic | Field options are now all, utm, or disable. |
| set logtraffic-start | New field. Enables logging of session start and end. |
| set netscan-discover-hosts | New field. Enables host discovery for hostname visibility feature. |
| set srcaddr6 | New fields. Set IPv6 addresses for source and destination. |
| set dstaddr6 | |
| set per-ip-shaper | This field is now also available for IPv6 policies. |
| set permit-any-host | New fields. These can help support the FaceTime application on NAT'd iPhones. |
| set permit-stun-host | |
| set require-tfa | New field. Makes identity-based policy require two-factor authentication. |
| set rso | New field. Enables RADIUS-based single sign on for this policy. |
| set send-deney-packet | New field. Enables sending a reply packet to denied TCP, UDP or ICMP traffic. If <code>deny-tcp-with-icmp</code> is enabled in system settings , a Communication Prohibited ICMP packet is sent. Otherwise, denied TCP traffic is sent a TCP reset. |
| set service-negate | New field. Negates service selection. |
| set srcaddr-negate | New field. Negates <code>srcaddr</code> selection. |
| set sso-auth-method | New field. Specifies passive authentication method for FSSO/RSSO. |
| set srcintf | Field now accepts multiple interface names. |
| set tcp-reset | Field removed. Use <code>send-deney-packet</code> instead. |
| set timeout-send-rst | New field. Enables sending a TCP reset when an application session times out. |
| set wanopt | New fields. Configure WAN Optimization on this policy. |
| set wanopt-detection | |
| set wanopt-profile | |
| set wanopt-peer | |
| set webcache-https | New field. Configures HTTPS web caching. |
| set wsso | New field. Enables WiFi Single Sign On. |
| config identity-based-policy | |
| edit <split_p_id> | |
| set action | New field. Selects the action for this policy. |
| set captive-portal | New field. Select the type of captive portal to use when <code>action</code> is <code>capture</code> . |
| set client-reputation | New field. Enables client reputation feature in policy. |
| set deep-inspection-options | New field. Applies a deep inspection options profile. |
| set devices | New field. Specifies the device categories to which the policy applies. |

| Command | Change |
|---|---|
| <pre> set endpoint-compliance set sslvpn-portal set sslvpn-realm set users </pre> | <p>New field. Enables endpoint compliance.</p> <p>New field. Selects the SSL VPN portal when <code>action</code> is <code>ssl-vpn</code>.</p> <p>New field. Specifies an SSL VPN realm for this policy.</p> <p>New fields. Selects individual users to add to the policy.</p> |
| <code>config firewall policy46, policy64</code> | New command. Configures IPv4 <-> IPv6 policies. |
| <code>config firewall profile-group</code> | |
| <pre> edit <group_name> set deep-inspection-options </pre> | New field. Applies a deep inspection options profile. |
| <code>config firewall profile-protocol-options</code> | |
| <pre> edit <name_str> set caname config dns config ftp set options bypass-mode-command set options bypass-rest-command config ftps config http set fortinet-bar set fortinet-bar-port set switching-protocols config https config imaps config pop3s config smtps config mapi </pre> | <p>Field moved from <code>firewall ssl setting</code>.</p> <p>New subcommand. Configures DNS protocol options.</p> <p>New option. Disables content scanning while <code>MODE</code> is 'block' or 'compressed'.</p> <p>New option. Disables content scanning while <code>REST</code> is not zero.</p> <p>Subcommand moved to <code>firewall deep-inspection-options</code>.</p> <p>New fields. Enable Fortinet Bar in browser.</p> <p>New field. Blocks or bypasses traffic when the protocol switches.</p> <p>Subcommands moved to <code>firewall deep-inspection-options</code>.</p> <p>New subcommand. Configures MAPI protocol options.</p> |
| <code>config firewall schedule onetime</code> | |
| <pre> edit <name_str> set expiration-days </pre> | New field. Sets time period for schedule expiry advance warning log entry. |
| <code>config firewall service category</code> | New command. Creates service categories and adds comments to service categories. Use <code>firewall service custom</code> to assign services to categories. |
| <code>config firewall service custom</code> | |
| <pre> edit <service_name> set category <category_name> set fqdn set iprange </pre> | <p>New field. Assigns the service to a service category.</p> <p>New field. Specifies FQDN for a service.</p> <p>New field. Specifies IP or IP range for a service.</p> |

| Command | Change |
|---|--|
| set explicit-proxy | New field. Configures a service as an explicit web proxy service. |
| set protocol {ALL CONNECT FTP HTTP SOCKS} | New set of options available when explicit-proxy is enabled. |
| set visibility | New field. Enables listing of service in firewall policy service selection. |
| config firewall service explicit-web | Command removed. Use firewall service custom with explicit-proxy enabled. |
| config firewall service group-explicit-web | Command removed. Use firewall service group with explicit-proxy enabled. |
| config firewall service group edit <group_name> set explicit-proxy | New field. Configures a service group as explicit web proxy services. |
| config firewall service predefined | Field removed. Use config firewall service custom. |
| config firewall sniffer | New command. Configures sniffer policies. |
| config firewall sniff-interface-policy edit <policy_id> set ips-DoS-status set ips-DoS set logtraffic | Fields removed. Use config firewall DoS-policy command. Field options are now all, utm, or disable. |
| config firewall sniff-interface-policy6 edit <policy_id> set logtraffic | Field options are now all, utm, or disable. |
| config firewall ssl setting set caname set ssl-max-version set ssl-min-version | Field moved to firewall profile-protocol-options . Fields removed. |
| config firewall ttl-policy | New command. Creates Generalized TTL Security Mechanism (GTSM) policies. |
| config firewall vip edit <name_str> set portmapping-type set srcintf-filter set ssl-algorithm custom config ssl-cipher-suites set weblogic-server set websphere-server | New field. Selects portmapping type. New field. Creates a source interface filter. New option. Enables custom encryption algorithm. New subcommand. Defines custom encryption algorithm. New field. Adds HTTP header indicating SSL offload for WebLogic server. New field. Adds HTTP header indicating SSL offload for WebSphere server. |
| config firewall vip6 | New command. Configures virtual IP addresses for IPv6. |

| Command | Change |
|---|---|
| config firewall vipgrp46 config firewall vipgrp64 | New commands. Configure vip46 and vip64 VIP groups. |
| config ips DoS | Command removed. Use config firewall DoS-policy , DoS-policy6 . |
| config ips global set algorithm super set database set skype-client-public-ipaddr | New option. Selects algorithm suitable for models with 4GB or more memory. New field. Selects regular or extended IPS database. New field. Defines network IP addresses used for Skype sessions to help identify Skype sessions in the Sessions dashboard widget. |
| config ips sensor set rate-count set rate-duration set rate-mode rate-track | New fields. Configure rate-based IPS signatures. |
| config log {disk fortianalyzer fortianalyzer2 fortianalyzer3 memory syslogd syslogd2 syslogd3 webtrends fortiguard} filter set analytics set endpoint set extended-traffic-log set suspicious set switching-protocols set voip set upload-format set web-filter-command-block | New field. Enables FortiGuard Analytics logging. Field moved from config log eventfilter . Field removed. Use log-invalid-packet in config log settings. New field. Enables virus suspicious logging. New field. Controls whether protocol switching is logged. Field moved from config log eventfilter . Field removed. Compact format no longer used. New field. Enables logging of web filter command block messages. |
| config log disk setting set maximum-log-age set max-policy-packet-capture-size set ms-per-transaction set report set rows-per-transaction set sql-max-size set sql-max-size-action set sql-oldest-entry set upload type voip | New field. Sets maximum age of log, after which it is purged. New field. Sets maximum size of packet captures in firewall policies. Field removed. New field. Enables reports. Fields removed. New option. Enables upload of VOIP logs. |

| Command | Change |
|--|--|
| config log eventfilter | |
| set amc-intf-bypass | Fields removed. Use system field. |
| set chassis-loadbalance-ha | |
| set cpu-memory-usage | |
| set ha | |
| set ldb-monitor | |
| set auth | Fields removed. Use user field. |
| set radius | |
| set config | Field removed. Use admin field. |
| set ipsec | Fields removed. Use vpn field. |
| set sslvpn-log-auth | |
| set sslvpn-log-adm | |
| set sslvpn-log-session | |
| set dhcp | Fields removed. Use network field. |
| set ppp | |
| set vip-ssl | |
| set gtp | |
| set notification | |
| set pattern | Fields removed. Use utm field. |
| set forticlient | |
| set mms-stats | |
| set nac-quarantine | Field removed. See endpoint in log {disk fortianalyzer fortianalyzer2 fortianalyzer3 memory syslogd syslogd2 syslogd3 webtrends fortiguard} filter |
| set network | New field. Enables logging of DHCP, PPP, VIP-SSL, GTP and notifications. |
| set voip | Field removed. See voip in log {disk fortianalyzer fortianalyzer2 fortianalyzer3 memory syslogd syslogd2 syslogd3 webtrends fortiguard} filter |
| set user | New field. Replaces auth and radius. |
| set utm | New field. Replaces pattern, forticlient, mms-stats, and nac-quarantine. |
| set vpn | New field. Replaces ipsec, sslvpn-log-auth, sslvpn-log-adm, sslvpn-log-session. |
| config log {fortianalyzer fortianalyzer2 fortianalyzer3} setting | |
| set buffer-max-send | Fields removed. Memory queue now used instead of file buffer. |
| set max-buffer-size | |
| set address-mode | Fields removed. Fortinet Discovery Protocol not supported in FortiOS 5.0 or FortiAnalyzer 5.0. |
| set fdp-device | |
| set fdp-interface | |

| Command | Change |
|---|---|
| config log fortiguard setting | |
| set source-ip | New field. Sets the source IP for communications to FAMS. |
| set upload-option | New field. Enables uploading logs to FortiGuard. |
| set upload-interval | New field. Sets frequency of log file upload. |
| set upload-time | New field. Sets the time to roll logs. |
| config log gui | Command removed. See <code>set gui-log-display</code> in <code>config system admin</code> . |
| config log gui-display | |
| set resolve-apps | Fields moved from config log setting . |
| set resolve-hosts | |
| config log memory setting | |
| set ips-archive | Command removed. DLP archive to memory is no longer supported. |
| config log setting | New command. Configures general logging settings. |
| set daemon-log | New field. Enables logging of daemons. |
| set gui-location | New field. Replaces <code>gui-log-location</code> in <code>system admin</code> . |
| set local-in-admin | New commands. Enable logging of local-in policies. |
| set local-in-deny | |
| set local-in-fortiguard | |
| set local-in-other | |
| set local-out | |
| set neighbor-event | New field. Enables logging of ARP and IPv6 neighbor discovery events. |
| set resolve-apps | Fields moved to config log gui-display . |
| set resolve-hosts | |
| set user-anonymize | New field. Enables anonymizing users as “anonymous” in logs. |
| config netscan settings | |
| set os-detection auto | Option renamed. <code>auto</code> was previously called <code>default</code> . |
| set service-detection auto | Option renamed. <code>auto</code> was previously called <code>default</code> . |
| set tcp-scan auto | Option renamed. <code>auto</code> was previously called <code>default</code> . |
| set udp-scan auto | Option renamed. <code>auto</code> was previously called <code>default</code> . |
| config report layout | |
| edit <layout_name> | |
| set schedule-type once | Option removed. Use <code>demand</code> option. |
| config body-item | |
| edit <item_id> | |
| set misc-component section-start | New option. Adds a report section. |
| config report summary | Command removed. No longer used. |

| Command | Change |
|--|---|
| config router bfd | New command. Enables BFD when there is no dynamic routing active. |
| config router bgp set ebgp-multipath set ibgp-multipath | New field. Enable ECMP load balancing across multiple (four) eBGP connections. New field. Enable ECMP load balancing across multiple (four) iBGP connections. |
| config router gwdetect edit <id> set gateway-ip set interface | Changed from edit <interface_name>. New field. Set gateway IP address. New field. Specifies interface. |
| config router multicast6 | New command. Configures the FortiGate unit as IPv6 Protocol Independent Multicast (PIM) version 2 router. |
| config router ospf config area config ospf-interface edit <ospf_interface_name> set network-type point-to-multipoint- non-broadcast set prefix-length | New network type option. New field. Sets size of OSPF hello prefix. |
| config router ospf6 config ospf6-interface edit <ospf6_interface_name> set network-type non-broadcast config neighbor | New network type option. New subcommand. |
| config router policy, policy6 | New command. Creates policy routes for IPv6 traffic. |
| config router ripng config distance | New subcommand. Similar to config distance subcommand in config router rip. |
| config spamfilter bwl | New command. Combines old emailbwl and ipbwl. |
| config spamfilter emailbwl | Command removed. Use config spamfilter bwl . |
| config spamfilter ipbwl | Command removed. Use config spamfilter bwl . |
| config spamfilter profile edit default set flow-based set spam-bwl-table set spam-emailbwl-table set spamipbwl-table config mapi | New field. Enables flow-based spam filtering. New field. Enables spam-bwl-table, which combines old spam-emailbwl-table and spamipbwl-table. Field removed. Use spam-bwl-table. Field removed. Use spam-bwl-table. New subcommand. Configures protocol options. |

| Command | Change |
|------------------------------------|---|
| config switch-controller | New command. Enables management of FortiSwitch units. |
| config system accprofile | |
| edit <profile-name> | |
| set fwgrp custom | |
| config fwgrp-permission | |
| set device | New field. Sets level of access to netscan device-identification configuration. |
| set utmpgrp custom | |
| config utmgrp-permission | |
| set voip | New field. Sets level of access to VOIP configuration. |
| config system admin | |
| edit <name_str> | |
| set guest-auth | New fields. Enable guest authentication and specify guest user groups. |
| set guest-groups | |
| set gui-detail-panel-location | Command removed. |
| set gui-log-display | Command removed. Replaced by gui-location in config log settings. |
| config dashboard | |
| edit n | |
| set widget-type sessions | |
| set report-by destination-location | Options removed. |
| set report-by destination-port | |
| edit n | |
| set widget-type sessions-bandwidth | |
| set sort-by | New options bandwidth and session. |
| config dashboard-tab | New subcommand. Configures additional dashboards. |
| config dashboard | |
| edit <id> | |
| set aggregate-hosts | New field. Enables host aggregation in Sessions widget. |
| set dst-interface | New field. Sets a destination filter for Sessions widget. |
| set show-forward-traffic | New field. Sets forward traffic filter for Sessions widget. |
| set show-local-traffic | New field. Sets local traffic filter for Sessions widget. |
| set show-policy-overflow | New field. Enables display of oversize policy alert in the Alert widget. |
| set widget-type analytics | New option. Selects the AntiVirus Statistics widget. |
| set widget threat-history | New option. Selects the Threat History widget. |
| config system alertemail | Renamed to config system email-server. |

| Command | Change |
|--|---|
| config system autoupdate clientoverride config system autoupdate override | Commands removed. Use the new central management override setting, fortimanager-fds-override, in config system central-management . |
| config system central-management set fortimanager-fds-override | New field. Enables FortiManager override of FDS server. Replaces set srv-ovrd and config srv-ovrd-lst in config system fortiguard. |
| config system console set login | New field. Disables console login. |
| config system ddns set ddns-server FortiGuardDDNS set monitor-interface | New option. Selects FortiGuard DDNS service. Option now supports multiple interfaces, allowing for failover. |
| config system dedicated-mgmt | New command. Configures dedicated management interface on model 100D. |
| config system dhcp server edit <server_index_int> set dns-service local set enable set ntp-server1 set ntp-server2 set ntp-server3 set ntp-service set option4 set option5 set option6 set status set vci-string set wifi-ac1 set wifi-ac2 set wifi-ac3 | New option. Use this FortiGate unit as a DNS server. Field renamed to status. New fields. Provide addresses of NTP servers. New field. Selects NTP source for DHCP clients. New fields. Provide additional custom DHCP options. Field renamed from enable. Field now supports multiple names separated by spaces, for example: set vci-string FortiAP FortiSwitch. New fields. Provide addresses of WiFi controllers. |
| config system elbc set inter-chassis-support set mode dual-forticontroller set mode forticontroller | New field. Enables content cluster inter-chassis support. New option. Supports FortiController. New option. Supports FortiController. |
| config system email-server set security set type | Renamed from config system alertemail. New field. Optionally selects STARTTLS or SMTPS security for email messages. Field removed. |

| Command | Change |
|---|--|
| config system fips-cc set entropy-token | New field. Enable to require USB entropy token for FIPS-CC boot-up. |
| config system fortiguard set analysis-service set ddns-server-ip set ddns-server-port set service-account-passwd set source-ip set srv-ovrd config srv-ovrd-lst set webfilter-sdns-server-ip set webfilter-sdns-server-port | Command removed. No longer required. New field. Sets IP for FortiDDNS service. New field. Sets port for FortiDDNS service. New field. Sets FAMS account password. Field moved from config system fortiguard-log command. Field and subcommand deleted. Use the new central management override setting, fortimanager-fds-override, in config system central-management. New fields. Sets the IP address and port of the FortiDNS server. |
| config system fortiguard-log | Command removed. See config log fortiguard setting . |
| config system fortisandbox | New command. Configure use of FortSandbox appliance. |
| config system geoip-override | New command. Configures overrides to IP geolocation database. |
| config system global set access-banner set admin-console-timeout set admin-https-redirect set admin-reset-button set allow-traffic-redirect set auth-lockout-duration set auth-lockout-threshold set block-session-timer set catutp-port set cert-chain-max set detection-summary set gui-certificates set gui-client-reputation set gui-dlp set gui-dynamic-routing | Field name changed to pre-login-banner. New field. Overrides admintimeout for console sessions. New field. Enables redirect of HTTP administrative access to HTTPS. New field. Disables unit reset button. New field. Stops redirection of traffic back out original interface. Fields moved to config user setting . New field. Sets duration for blocked sessions. New field. New field. Set maximum depth for a certificate chain. Field removed. Log & Archive Statistics widget removed from web-based manager. New field. Controls display of Certificate features in the web-based manager. New field. Controls display of client reputation features in the web-based manager. New field. Controls display of Data Leak Prevention features in the web-based manager. New field. Controls display of Dynamic Routing features in the web-based manager. |

| Command | Change |
|---|---|
| config system global (continued) | |
| set gui-explicit-proxy | New field. Controls display of Explicit Proxy features in the web-based manager. |
| set gui-implicit-id-based-policy | Field removed. Use set gui-implicit-policy. |
| set gui-multicast-policy | New field. Controls display of multicast policies in the web-based manager. |
| set gui-multiple-utm-profiles | New field. Controls display of multiple UTM profiles in the web-based manager. |
| set gui-nat46-64 | New field. Controls display of NAT46 and NAT64 settings in the web-based manager. |
| set gui-policy-based-ipsec | New field. Controls display of policy-based IPsec VPN options in the web-based manager. |
| set gui-replacement-message-groups | New field. Controls display of Replacement Message Groups in the web-based manager. |
| set gui-sslvpn-personal-bookmarks | New field. Controls display of Personal Bookmarks feature in the SSLVPN portal. |
| set gui-sslvpn-realms | New field. Controls display of SSL VPN realms in the web-based manager. |
| set gui-utm-monitors | New field. Controls display of UTM monitors in the web-based manager. |
| set gui-wanopt-cache | New field. Controls display of WANopt features in the web-based manager. |
| set gui-wireless-opensecurity | New field. Controls display of open security option for SSID in the web-based manager. |
| set login-timestamp | New field. Controls logging of login timestamps. |
| set max-dlpstat-memory | New field. Controls amount of memory DLP stat daemon uses. |
| set max-report-db-size | New field. Sets the maximum size for the log report database. |
| set max-sql-log-size | Field removed. |
| set miglogd-children | New field. Sets the number of miglogd process to run. |
| set optimize-ssl | New field. Enables optimization of SSL inspection by using multiple processes. |
| set per-user-bwl | New field. Enables webfilter per-user black/white list. |
| set policy-auth-concurrent <limit_int> | Field changed to numerical limit, or 0 for no limit. |
| set post-login-banner | New field. Enables disclaimer message that appears after login. |
| set pre-login-banner | Field name changed. Was access-banner. |
| set revision-backup-on-logout | Default changed to disable. |
| set revision-image-auto-backup | New field. Enables auto-backup of image on upgrade. |
| set sslvpn-cipher-hardware-acceleration | New fields. Control hardware acceleration for SSLVPN. |
| set sslvpn-kxp-hardware-acceleration | |
| set sslvpn-pkce2-hardware-acceleration | New field. Controls PKCE2 hardware acceleration for SSLVPN. |
| set sslvpn-personal-bookmarks | New field. Enables management of SSLVPN user bookmarks in the web-based manager. |

| Command | Change |
|---|--|
| config system global (continued) | |
| set ssl-worker-count | New field. Sets number of processes to use for optimization of SSL inspection. |
| set switch-controller | New field. Enables switch controller on models where switch management is supported. |
| set switch-controller-reserved-network | New field. Defines a subnet for managed switches. |
| set two-factor-email-expiry | New field. Sets the timeout period for email-based two-factor authentication. |
| set two-factor-sms-expiry | New field. Sets the timeout period for SMS-based two-factor authentication. |
| set usb-wan-auth-type | New fields. Set authentication parameters for 4G/LTE modems. |
| set usb-wan-extra-init | |
| set usb-wan-passwd | |
| set usb-wan-username | |
| set use-usb-wan | New field. Enables use of USB wireless LTE modem. |
| set virtual-server-hardware-acceleration | New fields. Control hardware acceleration. |
| set virtual-server-count | |
| set wan | New field. On models FWF-20C-ADSL and FGT-20C-ADSL enables one of the switch port interfaces to act as a WAN port. |
| set wireless-controller | New field. Disables wireless daemon. |
| set wireless-mode wtp | Option removed. |
| config system ha | |
| set gratuitous-arps | New field. Disables gratuitous ARP packets from new master unit. |
| set group-id | Value range now 0-255. |
| set minimum-worker-threshold | New field. Defines threshold to assign a lower rank to systems with few worker blades when electing an HA master. |
| set update-all-session-timer | New field. Enables updating all session timers after a failover. |
| config frup-settings | New subcommand. Configures Fortinet Redundant UTM Protocol (FRUP). |
| config system interface | |
| edit <interface_name> | |
| set allowaccess dynamic-profile-radius-server | Field name changed to radius-acct. |
| set allowaccess radius-acct | Field renamed, was dynamic-profile-radius-server. |
| set allowaccess capwap | New option. Enables CAPWAP data on interface. |
| set atm-protocol | New field. Enables IPoA protocol on ADSL interfaces that support it. |
| set dedicate-to | New field. Dedicates mgmt interface to unit management, optionally limited to trusted source IPs. |

| Command | Change |
|--|--|
| config system interface (continued) | |
| set dedicate-to-switch | New field. |
| set device-access-list | New field. Selects a device access list when device-identification is enabled. |
| set device-identification | New field. Enables discovery of OS and device information for source hosts. |
| set device-netscan | New field. Enables inclusion of detected devices in network vulnerability scans. |
| set device-user-identification | New field. Enables determination of user name for source hosts. |
| set drop-fragment | New field. Enables dropping and logging of fragmented packets. |
| set dropped-overlapped-fragment | New field. Enables dropping of overlapped packet fragments. |
| set listen-forticlient-connection | New field. Enables interface listening for connecting FortiClient endpoints. |
| set log | Field removed. |
| set replacemsg-override-group | New field. Selects replacement message override group for captive portal messages. |
| set security-groups | New field. Selects groups that can get access through captive portal on this interface. |
| set security-mode | New field. Selects security mode for interface. |
| set snmp-index | New field. Specifies interface index value for SNMP. |
| set stpforward-mode | New field. Sets Spanning Tree Protocol forwarding mode. |
| set trust-ip-1 | New fields. When dedicate-to is management, these fields specify trusted IP addresses for management access. |
| set trust-ip-2 | |
| set trust-ip-3 | |
| set wifi-auto-connect | New field. Makes client mode WiFi automatically connect to nearest saved WiFi network. |
| set wifi-auto-save | New field. Makes client mode WiFi automatically save passphrase when it connects to a WiFi network. |
| config ip6 | |
| set dhcp6-relay-server | New fields. Configure DHCP relay server for IPv6. |
| set dhcp6-relay-ip | |
| set ip6-mode | New field. Selects static or DHCP6 addressing. |
| config wifi-networks | New subcommand. Configures settings for WiFi in client mode. |
| config system ipip-tunnel | New command. Configures RFC 1853 IP-to-IP tunnel. |
| config system ips-urlfilter-dns | New command. Configures IPS URL filter DNS servers. |
| config system ipv6-neighbor-cache | New command. Saves neighbor cache entries for the VDOM. |

| Command | Change |
|---|---|
| config system mac-address-table edit <mac-address_hex> set reply-substitute | New field. Defines a substitute MAC address to use in reply. |
| config system modem set lockdown-lac set network-init | New command. Allows connection only to the specified location area code (LAC). New command. Sets current GSM/UMTS network operator. |
| config system nat64 | New command. Configures NAT64 (communication between IPv6 hosts and IPv4 servers). |
| config system network-visibility | New command. Configures network visibility features. |
| config system np6 | New command. Configures the NP6 and NPlite Network Processing Unit (NPU). |
| config system npu set dedicated-management-cpu set dedicated-tx-npu | New field (some models). Enables dedicating one CPU to management functions. New field. On model 3600C, enables slow path packet processing using a dedicated third NP4. |
| config system ntp set type set server-mode set interface | New field. Selects either FortiGuard or custom NTP server definition. New fields. Configure an NTP server to be available on specified interfaces. |
| config system npu set elbc-mode | Field removed. Use mode field in config system elbc . |
| config system probe-response | New command. Configures response to server probing. |
| config system replacemsg auth auth-token-login | New command, Defines replacement message for two-factor authentication. |
| config system replacemsg auth auth-token-login-failed | New command. Defines replacement message when two-factor authentication fails. |
| config system replacemsg device-detection-portal device-detection-failed | New command. Defines replacement message when FortiGate unit cannot identify device type. |
| config system replacemsg ftp ftp-dl-dlp config system replacemsg ftp ftp-dl-infected | Commands removed. See system replacemsg utm . |
| config system replacemsg http http-client-virus config system replacemsg http http-dlp config system replacemsg http http-virus | Commands removed. See system replacemsg utm . |
| config system replacemsg mail email-dlp config system replacemsg mail email-virus config system replacemsg mail smtp-virus | Commands removed. See system replacemsg utm . |

| Command | Change |
|--|--|
| config system replacemsg nntp nntp-dl-infected | Commands removed. See system replacemsg utm . |
| config system replacemsg nntp nntp-dlp | |
| config system replacemsg utm | New command. Replacement messages for some FTP, HTTP, and email data leak and virus detections. |
| config system server-probe | New command. Configures server probing. |
| config system session-sync edit <sync_id> config filter set service set dstaddr6 set srcaddr6 config custom-service | Field removed. Use custom-service subcommand. New fields. Set IPv6 addresses for session sync destination and source. New subcommand. Configures custom service filter. Replaces service field. |
| config system settings set deny-tcp-with-icmp set discovered-device-timeout set email-portal-check-dns set gui-default-policy-columns set mac-ttl set ses-denied-traffic set sip-ssl-port set tcp-port | New field. Enables denying TCP, UDP or ICMP traffic by sending an ICMP Communication Prohibited packet. New field. Sets timeout of discovered devices. New field. Enables email collection portal checking of user-supplied email domains. New field. Overrides firewall policy displayed column set. New field. Sets duration of MAC addresses in transparent mode. New field. Enables inclusion of denied traffic in the session table. New field. Sets the port that the SIP proxy monitors for SIP traffic. Field now accepts two port numbers. |
| config system sflow set source-ip | New field. Sets IP address for sFlow agent. |
| config system sms-server | New command. Defines SMS servers for use in two-factor authentication. |
| config system snmp community edit <index_number> set events fan-failure | New option. Enables fan failure event. |
| config system snmp user edit <user_name> set events fan-failure config hosts edit <host_id> set host-type | New option. Enables fan failure event. New field. Determines permitted SNMP actions for host. |

| Command | Change |
|--|--|
| config system stp | New command. Configures STP on Internal interface switches in switch mode. |
| config system vdom-link edit <name> set type | New field. Selects type of VDOM link: PPP or Ethernet. |
| config system vdom-radius-server | New command. Specifies the dynamic profile RADIUS server for each VDOM. |
| config system virtual-switch | New command. Configures virtual switch interfaces. |
| config user device | New command. Defines devices. |
| config user device-access-list | New command. Configures device lists for use on interfaces with device identification enabled. |
| config user device-category | New command. Displays comments and descriptions for predefined device types. |
| config user device-group | New command. Defines device groups. |
| config user fortitoken edit <serial_number> set activation-code set activation-expire set license | New fields to support FortiToken Mobile soft token. |
| config user fsso-polling | New command. Configures polling of Windows AD servers. |
| config user group edit <groupname> set auth-concurrent-override set auth-concurrent-value set company set email set mobile-phone set password set sponsor set user-id set user-name set expire <seconds_int> set expire-type set group-type fsso-service set group-type guest set group-type rsso set multiple-guest-add set sslvpn-portal set sso-attribute-value | <p>New fields. Override policy-auth-concurrent setting in system global.</p> <p>New fields. When <code>group-type</code> is <code>guest</code>, these fields enable or disable fields on the web-based manager Guest Management page. The <code>user-id</code> and <code>password</code> fields can select either an auto-generated value, an email address, or a specified value.</p> <p>New fields. When <code>group-type</code> is <code>guest</code>, these fields specify the time until account expiry beginning either immediately or after the user's first login.</p> <p>Value renamed from <code>directory-service</code>.</p> <p>New value. Guest user groups are used for guest WiFi accounts.</p> <p>New value. RADIUS SSO users.</p> <p>New field. Enables auto-creation of a number of guest user accounts.</p> <p>Field removed. Use identity-based firewall policy <code>sslvpn-portal</code> field.</p> <p>New field. Defines the RADIUS user group that this local user group represents.</p> |

| Command | Change |
|---|---|
| <pre> config guest config match edit <id> set rspo </pre> | <p>New subcommand. Configures guest user.</p> <p>New field. Enables RSO match in this group.</p> |
| <pre> config user ldap edit <server_name> set source-ip set secondary-server set tertiary-server </pre> | <p>New field. Specifies an IP address to use for LDAP communications.</p> <p>New field. Specifies a secondary LDAP server to use if the primary server is unavailable.</p> <p>New field. Specifies a tertiary LDAP server to use if both the primary and secondary servers are unavailable.</p> |
| <pre> config user local edit <name> set auth-concurrent-override set auth-concurrent-value set passwd-policy set sms-custom-server set sms-phone set sms-server set two-factor set workstation </pre> | <p>New fields. Override policy-auth-concurrent setting in system global.</p> <p>New field. Applies a password policy to this account.</p> <p>New fields. Configure two-factor authentication.</p> <p>New field. Limits user logon to a specified workstation.</p> |
| <pre> config user password-policy </pre> | <p>New command. Creates a user password policy.</p> |
| <pre> config user peer edit <peer_name> set ocsp-override-server <ocsp_name> </pre> | <p>New field. Sets OCSP server to use to retrieve certificate, if OCSP is enabled.</p> |
| <pre> config user radius edit <server_name> set dynamic-profile set dp-* </pre> | <p>Fields removed. The RADIUS SSO feature replaces the dynamic profile feature. Use <code>rsso-*</code> fields.</p> |

Command

```
set h3c-compatibility
set rso
set rso-radius-server-port
set rso-radius-response
set rso-validate-request-secret
set rso-secret
set rso-endpoint-attribute
set rso-endpoint-block-attribute
set rso-context-timeout
set rso-log-period
set rso-log-flags
set rso-flush-ip-session
set sso-attribute
set sso-attribute-key
set secondary-server
set secondary-secret
set tertiary-server
set tertiary-secret
config accounting-server
```

Change

New field. Enables compatibility with H3C Intelligent Management Platform (IMC) server.

New fields for RADIUS SSO feature that replaces Dynamic Policy feature.

New fields. Specify a secondary RADIUS server to use if the primary server is unavailable.

New fields. Specify a tertiary RADIUS server to use if both the primary and secondary are unavailable.

New subcommand. Configures accounting server.

config `user setting`

```
set auth-lockout-duration
set auth-lockout-threshold
set auth-timeout
set radius-ses-timeout-act
```

Fields moved from `config system global`.

Maximum is now 1440 minutes (24 hours).

New field. Selects whether to use or ignore RADIUS session timeout.

config `user tacacs+`

```
edit <server_name>
set secondary-server
set secondary-key
set tertiary-server
set tertiary-key
```

New fields. Specifies a secondary TACACS+ server to use if the primary server is unavailable.

New fields. Specifies a tertiary TACACS+ server to use if both the primary and secondary servers are unavailable.

| Command | Change |
|--|---|
| <pre>config voip profile edit <profile_name> set extended-utm-log config sip set open-record-route-pinhole set open-via-pinhole set ssl-mode set ssl-algorithm set ssl-auth-client set ssl-auth-server set ssl-client-certificate set ssl-client-renegotiation set ssl-min-version set ssl-max-version set ssl-pfs set ssl-send-empty-frags set ssl-server-certificate</pre> | <p>New field. Enables detailed UTM log messages.</p> <p>New SIP-related commands.</p> <p>New SSL-related commands for models equipped with CP6, CP7, or CP8 processor.</p> |
| <pre>config vpn certificate ca edit <ca_name> set source-ip</pre> | <p>New field. Defines expected IP for requests.</p> |
| <pre>config vpn certificate crl edit <ca_name> set source-ip</pre> | <p>New field. Defines expected IP for requests.</p> |
| <pre>config vpn certificate local edit <ca_name> set source-ip</pre> | <p>New field. Defines expected IP for requests.</p> |
| <pre>config vpn certificate ocsdp-server edit <ca_name> set source-ip</pre> | <p>The config vpn certificate ocsdp command was re-organized to support multiple servers.</p> <p>New field. Defines expected IP for requests.</p> |
| <pre>config vpn certificate setting</pre> | <p>New command. Enables obtaining certificates by OSCP and setting default server.</p> |
| <pre>config vpn ipsec manualkey edit <tunnel_name> set encryption aria128 set encryption aria192 set encryption aria256 set encryption seed set npu-offload</pre> | <p>New options. ARIA is a Korean 128-bit block algorithm with a 128, 192, or 256-bit key. SEED is a Korean 128-bit block algorithm with a 128-bit key.</p> <p>New field. Enables offload of VPN session to NPU.</p> |
| <pre>config vpn ipsec manualkey-interface edit <tunnel_name> set enc-alg aria128 set enc-alg aria192 set enc-alg aria256 set enc-alg seed</pre> | <p>New options. ARIA is a Korean 128-bit block algorithm with a 128, 192, or 256-bit key. SEED is a Korean 128-bit block algorithm with a 128-bit key.</p> |

| Command | Change |
|--|---|
| set npu-offload | New field. Enables offload of VPN session to NPU. |
| config vpn ipsec phase1 | |
| edit <gateway_name> | |
| set autoconfig | New field. Enables VPN autoconfiguration as a gateway or a client. |
| set fragmentation | New field. Enables IKE fragmentation support. |
| set ike-version | New field. Selects either IKE v1 or v2. Previously only phase1-interface supported v2. |
| set proposal aria128 | New options. ARIA is a Korean 128-bit block algorithm with a 128, 192, or 256-bit key. SEED is a Korean 128-bit block algorithm with a 128-bit key. |
| set proposal aria192 | |
| set proposal aria256 | |
| set proposal seed | |
| set xauthexpire | New field. Controls when XAUTH credentials expire. |
| config vpn ipsec phase1-interface | |
| edit <gateway_name> | |
| set client-auto-negotiate | New field. Enables client to bring up the tunnel when there is no traffic. |
| set client-keep-alive | New field. Enables client to keep the tunnel up when there is no traffic. |
| set fragmentation | New field. Enables IKE fragmentation support. |
| set include-local-lan | New field. Enables access to their local LAN for Unity users who are not using split tunneling. |
| set monitor | Field renamed from monitor-phase1. |
| set monitor-phase1 | Field renamed to monitor. |
| set monitor-hold-down-delay | New field. Sets time to delay return to primary interface from backup interface. |
| set npu-offload | New field. Controls offload of VPN session to NPU. |
| set proposal aria128 | New options. ARIA is a Korean 128-bit block algorithm with a 128, 192, or 256-bit key. SEED is a Korean 128-bit block algorithm with a 128-bit key. |
| set proposal aria192 | |
| set proposal aria256 | |
| set proposal seed | |
| set save-password | New field. Enables FortiClient users to save Xauth user name and password. |
| set send-cert-chain | New field. Enables sending of certificate chain, rather than single certificate. |
| set split-include-service | New field. Determines which services the client can access through the VPN. |
| set xauthexpire | New field. Controls when XAUTH credentials expire. |
| config vpn ipsec phase2 | |
| edit <tunnel_name> | |
| set l2tp | New field. Enables L2TP traffic over IPsec VPN. |
| set proposal aria128 | New options. ARIA is a Korean 128-bit block algorithm with a 128, 192, or 256-bit key. SEED is a Korean 128-bit block algorithm with a 128-bit key. |
| set proposal aria192 | |
| set proposal aria256 | |
| set proposal seed | |

| Command | Change |
|---|--|
| <pre> config vpn ipsec phase2-interface edit <tunnel_name> set l2tp set proposal aria128 set proposal aria192 set proposal aria256 set proposal seed </pre> | <p>New field. Enables L2TP traffic over IPsec VPN.</p> <p>New options. ARIA is a Korean 128-bit block algorithm with a 128, 192, or 256-bit key. SEED is a Korean 128-bit block algorithm with a 128-bit key.</p> |
| <pre> config vpn ssl settings set allow-ssl-big-buffer set allow-ssl-insert-empty-fragment set allow-ssl-client-renegotiation set auto-tunnel-policy set auto-tunnel-static-route set dns-suffix set http-only-cookie set port-precedence set tlsv1-0 set tlsv1-1 set tlsv1-2 </pre> | <p>New fields. Default settings enhance performance.</p> <p>New field. Controls renegotiation of SSL connection.</p> <p>New field. Enables automatic creation of policies for SSLVPN.</p> <p>New field. Enables automatic creation of static routes for SSLVPN.</p> <p>New field. Adds DNS suffix support for SSLVPN tunnel mode.</p> <p>New field. Disables httponly cookie.</p> <p>New field. Enables giving SSLVPN higher priority than HTTPS if both are enabled on the same port.</p> <p>New fields. Enable TLS v1.0, 1.1, and 1.2 protocols.</p> |
| <pre> config vpn ssl web portal edit <portal_name> set auto-prompt-mobile-user set mac-addr-action set mac-addr-check config mac-addr-check-rule edit "rule1" set mac-addr-list set mac-addr-mask end config os-check-list windows-8 config widget edit <widget_id> set type forticlient-download set auto-connect set keep-alive set save-password set type history set type tunnel set tunnel-status </pre> | <p>New field. Enables prompt for mobile users to download FortiClient Endpoint Security.</p> <p>New fields. Define MAC address host checking.</p> <p>New option for os-check-list.</p> <p>Widget configuration.</p> <p>New option. Creates widget for downloading FortiClient Endpoint Security.</p> <p>New fields. Options for FortiClient users.</p> <p>New option. Creates login history widget.</p> <p>Option removed.</p> |

| Command | Change |
|--|---|
| <pre> set dns-server1 set dns-server2 set ipv6-dns-server1 set ipv6-dns-server2 set ipv6-wins-server1 set ipv6-wins-server2 set wins-server1 set wins-server2 config bookmarks edit <bookmark_name> set sso static set sso-credential set sso-username set sso-password </pre> | <p>New fields for tunnel widget.</p> <p>Option removed. Use <code>auto</code> option and set <code>sso-credential</code> to alternative.</p> <p>New field. Selects SSL-VPN or alternative credentials.</p> <p>New fields. Specify alternative credentials for a bookmark.</p> |
| <code>config vpn ssl web realm</code> | New command. Configures SSL VPN realms. |
| <pre> config vpn ssl web user edit <user_name> config widget edit <widget_id> config bookmarks edit <bookmark_name> set sso auto set sso-credential set sso-username set sso-password </pre> | <p>New field. Selects SSL-VPN or alternative credentials.</p> <p>New fields. Specify alternative credentials for a bookmark.</p> |
| <code>config wanopt rule</code> | Command replaced by <code>config wanopt profile</code> . |
| <code>config wanopt profile</code> | New command. Replaces <code>config wanopt rule</code> . |
| <pre> config wanopt settings edit <ssl-server-name> set add-header-x-forwarded-proto </pre> | New field. Adds X-Forwarded_Proto header. |
| <pre> config wanopt ssl-server edit <ssl-server-name> set ssl-client-renegotiation set url-rewrite </pre> | <p>New field. Controls client renegotiation.</p> <p>New field. Enables rewrite of HTTP redirection Location header.</p> |
| <pre> config wanopt webcache set cache-cookie set cache-exemption config cache-exemption-list </pre> | <p>New field. Enables cookie caching.</p> <p>Field moved to <code>web-proxy url-match</code>.</p> <p>Subcommand removed. Use <code>web-proxy url-match</code>.</p> |

| Command | Change |
|--|--|
| <pre>config web-proxy explicit set ipv6-status set incoming-ip6 set outgoing-ip6 set ssl-algorithm</pre> | <p>New fields. Configure IPv6 explicit web-proxy.</p> <p>New field. Sets the strength of encryption algorithms accepted for deep scan.</p> |
| <pre>config web-proxy forward-server-group</pre> | <p>New command. Configures a load-balanced group of web proxy forward servers.</p> |
| <pre>config web-proxy global set forward-server-affinity-timeout set tunnel-non-http set unknown-http-version</pre> | <p>New field. Sets affinity timeout for load balancing in a forward server group.</p> <p>New field. Enables non-HTTP tunneling.</p> <p>New field. Selects how to handle requests with unknown HTTP version.</p> |
| <pre>config web-proxy url-match</pre> | <p>New command. Defines URLs for forward-matching or cache exemption.</p> |
| <pre>config webfilter content-header edit <entry_number> config entries edit <regex> set category</pre> | <p>New field. Specifies FortiGuard categories to match.</p> |
| <pre>config webfilter ips-urlfilter-cache-setting</pre> | <p>New command. Configures the global DNS settings for flow-based URL filtering in conjunction with a border gateway.</p> |
| <pre>config webfilter ips-urlfilter-setting</pre> | <p>New command. Configures a gateway router to do flow-based url filtering.</p> |
| <pre>config webfilter profile edit <name_str> set extended-utm-log set log-all-url set options per-user-bwl set web-filter-activex set web-filter-activex-log set web-filter-command-block-log set web-filter-sdns-action set web-filter-sdns-portal</pre> | <p>New field. Enables detailed UTM log messages.</p> <p>New field. Enables logging of all URLs, even if FortiGuard is not enabled.</p> <p>New option. Enables per-user black/white list.</p> <p>Renamed option. web-filter-activex renamed to web-filter-activex-log for consistency.</p> <p>New field. Enables logging of web filter command block messages.</p> <p>New fields. Configures redirection to a captive portal by FortiGuard DNS-based web filtering.</p> |

| Command | Change |
|---|--|
| <pre> config ftgd-wf set disable set enable set category-override config quota edit <id> set type {time traffic} set unit set value config web set log-search set safe-search set youtube-edu-filter-id </pre> | <p>Field removed as it was redundant with enable field.</p> <p>Field renamed to category-override.</p> <p>Field renamed from enable.</p> <p>New fields. Configure traffic quotas.</p> <p>New field. Enables logging of all search words.</p> <p>Field changed. Now selects whether safe search is based on the request URL or header.</p> <p>New field. Sets YouTube EDU ID.</p> |
| config webfilter search-engine | New command. Configures search engine access. |
| <pre> config webfilter urlfilter edit <list_int> set one-arm-ips-urlfilter </pre> | New field. Enables IPS URL filter. |
| <pre> config wireless-controller global set max-discoveries set ac-discovery-type set ac-list set ac-port set discovery-mc-ttl set image-update set max-failed-dtls set mesh-eth-type </pre> | <p>Fields removed. These were used when a FortiWiFi unit runs in WTP mode, which is not supported in FortiOS 5.0.</p> <p>New field. Sets mesh ID for use in packets.</p> |
| <pre> config wireless-controller setting set ap-auto-suppress set ap-bgscan-period set ap-bgscan-disable-day set ap-bgscan-disable-start set ap-bgscan-disable-end </pre> | <p>New field. Enables automatic suppression of detected rogue APs.</p> <p>New field. Sets interval between background scans.</p> <p>New fields. Configure a period on one or more days of the week when background scanning is disabled.</p> |
| <pre> config wireless-controller timers set fake-ap-log </pre> | New field. Sets reporting interval for fake AP log. |
| <pre> config wireless-controller vap edit <vap_name> set broadcast-suppress [arp dhcp] set dynamic-vlan set external-fast-roaming </pre> | <p>New field. Prevents ARP or DHCP messages being carried to other access points carrying the same SSID.</p> <p>New field. Enables user VLAN assignment based on RADIUS attribute.</p> <p>New field. Enables pre-authentication with external non-managed AP.</p> |

| Command | Change |
|--|---|
| <pre> set gtk-rekey-intv set ptk-rekey-intv set multicast-enhance set me-disable-thresh set local-bridging set local-switching set mesh-backhaul set vlanid set radius-mac-auth set radius-mac-auth-server set mac set mac-filter set mac-filter-policy set mac-filter-policy-other config mac-filter-list set vlan-auto </pre> | <p>New fields. Modify WPA and WPA-RADIUS rekey intervals.</p> <p>New fields. Enable conversion of multicast to unicast to improve performance, with an upper limit.</p> <p>New field. Enables bridging WiFi and Ethernet interfaces.</p> <p>New field. Enables bridging VAP interfaces.</p> <p>New field. Enables SSID as backhaul link.</p> <p>New field. Sets VLAN ID.</p> <p>New fields. Configure MAC-based authentication of WiFi clients on a RADIUS server.</p> <p>Subcommand removed. Use DHCP server reserved-address capability.</p> <p>New field. Enables automatic management of SSID VLAN interface.</p> |
| <pre>config wireless-controller vap-group</pre> | Command removed. |
| <pre>config wireless-controller wids-profile</pre> | New command. Configures profiles for the Wireless Intrusion Detection System (WIDS). |
| <pre> config wireless-controller wtp edit <wtp-id> set auto-power-level set auto-power-low set auto-power-high set band set ip-fragment-preventing set tun-mtu-downlink set tun-mtu-uplink config lan </pre> | <p>New fields. Configure automatic power adjustment to prevent interference.</p> <p>New field. Select radio band to use with automatic profile.</p> <p>New field. Enables methods of CAPWAP fragmentation prevention, including MTU adjustment.</p> <p>New fields. Adjust CAPWAP MTU.</p> <p>New subcommand. Controls use of FortiAP LAN ports.</p> |
| <pre> config wireless-controller wtp-profile edit <name_str> set ap-country set dtls-enabled set handoff-rssi set handoff-sta-thresh set ip-fragment-preventing set max-clients </pre> | <p>New field. Sets country of AP operation.</p> <p>New field. Enables DTLS encryption for CAPWAP data channel.</p> <p>New field. Sets minimum RSSI threshold for handoff.</p> <p>New field. Sets threshold value for AP handoff.</p> <p>New field. Enables methods of CAPWAP fragmentation prevention, including MTU adjustment.</p> <p>New field. Sets a maximum number of clients that the AP will support.</p> |

Command

```
set tun-mtu-downlink
set tun-mtu-uplink
config lan
config radio-1, radio-2
    set ap-auto-suppress
    set ap-bgscan-period
    set ap-bgscan-disable-day
    set ap-bgscan-disable-start
    set ap-bgscan-disable-end
    set ap-handoff

    set auto-power-level
    set auto-power-low
    set auto-power-high
    set frequency-handoff

    set max-distance

    set protection-mode
    set station-locate
    set wids-profile
```

Change

New fields. Adjust CAPWAP MTU.

New subcommand. Controls use of FortiAP LAN ports.

New field. Enables automatic rogue suppression.

New field. Sets interval between background scans.

New fields. Configure a period on one or more days of the week when background scanning is disabled.

New field. Enables controller to switch clients to another AP for load balancing.

New fields. Configure automatic power adjustment to prevent interference.

New field. Enables controller to switch clients to the other frequency band (2.4GHz or 5GHz) for load balancing.

New field. Adjusts AP for optimum throughput at the specified distance.

New field. Enables 802.11g protection.

New field. Enables station location service.

New field. Assigns WIDS profile to this radio.

`execute backup config usb-mode`

New command. Backs up configuration to a USB drive, which can be encrypted with a password.

`execute central-mgmt update`

Command removed. No longer required.

`execute client-reputation erase`
`execute client-reputation host-count`
`execute client-reputation host-detail`
`execute client-reputation host-summary`
`execute client-reputation purge`
`execute client-reputation topN`

New commands to view and remove client reputation information.

`execute erase-disk`

New command. Reformats boot device or other hard drive. Optionally, can restore image afterwards.

`execute factoryreset2`

New command. Resets the FortiGate configuration to factory default settings except VDOM and interface settings.

`execute factoryreset [keepvmlicense]`
`execute factoryreset2 [keepvmlicense]`

New option. Preserves VM license after reset. Available on VM models only.

`execute firmware-list update`

Command removed. No longer required.

`execute forticarrier-license`

New command. Updates FortiCarrier license.

`execute fortiguard-log agreement`
`execute fortiguard-log certification`
`execute fortiguard-log create-account`
`execute fortiguard-log login`

New commands for managing the FortiCloud account.

| Command | Change |
|---|---|
| <code>execute fortisandbox test-connectivity</code> | New command. Queries connectivity to FortiSandbox appliance . |
| <code>execute fortitoken import</code> | New command. Imports OTP seeds. |
| <code>execute fortitoken-mobile import</code> <code>execute fortitoken-mobile poll</code> <code>execute fortitoken-mobile provision</code> | New commands. Configure FortiToken Mobile soft tokens. |
| <code>execute ha ignore-hardware-revision</code> | New command. Sets ignore-hardware-revision status. |
| <code>exec ha sync avupd</code> <code>exec ha sync attackdef</code> <code>exec ha sync weblists</code> <code>exec ha sync emaillists</code> <code>exec ha sync ca</code> <code>exec ha sync localcert</code> <code>exec ha sync ase</code> <code>exec ha sync all</code> | Obsolete commands removed. |
| <code>execute log convert-oldlogs</code> <code>execute log delete-oldlogs</code> | New commands. Available only if your system contains old compact logs created by an earlier version of FortiOS. |
| <code>execute log filter reset field</code> | New option. Resets only log filter fields. |
| <code>execute log upload-progress</code> | New command. Displays progress of latest log upload. |
| <code>execute netscan start discover</code> | Command removed. |
| <code>execute policy-packet-capture delete-all</code> | New command. Deletes captured packets. |
| <code>execute report flash-cache</code> | New command. Generates cache record in the report database. |
| <code>execute report run</code> | Command modified. Now accepts start and end times. |
| <code>execute restore config usb-mode</code> | New command. Restores configuration from a USB drive, which can be encrypted with a password. |
| <code>execute restore src-vis</code> | New command. Download source visibility signature package. |
| <code>execute ssh <destination> [<port>]</code> | New option to specify port number. |
| <code>execute sync-session</code> | New command. Forces session synchronization |
| <code>execute update-geo-ip</code> | New command. Updates the IP geography database from FortiGuard. |
| <code>execute update-modem</code> | Command removed. No longer required. |
| <code>execute update-src-vis</code> | New command. trigger an FDS update of the source visibility signature package. |
| <code>execute usb-device {list disconnect}</code> | New commands. Manage FortiExplorer IOS devices. |
| <code>execute webfilter quota-reset</code> | New command. Resets user webfilter quota. |
| <code>get log sql status</code> | Command removed. |
| <code>get mgmt-data status</code> | New command. Displays information additional to that provided by <code>get system status</code> or <code>get hardware status</code> . |
| <code>get netscan scan</code> | Command removed. |
| <code>get router route6</code> | New command. Lists IPv6 policy routes. |

| Command | Change |
|--|---|
| <code>get system fdp-fortianalyzer</code> | Command removed. Fortinet Discovery Protocol not supported in FortiOS 5.0 or FortiAnalyzer 5.0. |
| <code>get wireless-controller rf-analysis</code> | New command. Provides information about radio conditions on each channel at an AP. |
| <code>get wireless-controller status</code> | New command. Shows the numbers of wtp sessions and clients. |
| <code>get wireless-controller vap-status</code> | New command. Shows information about SSIDs. |
| <code>get wireless-controller wlchanlistlic</code> | New command. Shows radio channels information. |
| <code>get wireless-controller wtp-status</code> | New command. Returns information about an AP. |

alertemail

Use the `config alertemail` command to configure the FortiGate unit to monitor logs for log messages with certain severity levels. If the message appears in the logs, the FortiGate unit sends an email to predefined recipients of the log message encountered. Alert emails provide immediate notification of issues occurring on the FortiGate unit, such as system failures or network attacks.



You must configure the server setting under `config system email-server` before the commands under `config alertemail` become accessible.

This chapter describes the following command:

[setting](#)

setting

Use this command to configure the FortiGate unit to send an alert email to up to three recipients. This command can also be configured to send an alert email a certain number of days before the FDS license expires and/or when the disk usage exceeds a certain threshold amount. You need to configure an SMTP server before configuring alert email settings. See [“system email-server” on page 514](#) for more information.

Syntax

```
config alertemail setting
    set username <user-name_str>
    set mailto1 <email-address_str>
    set mailto2 <email-address_str>
    set mailto3 <email-address_str>
    set filter-mode {category | threshold}
    set email-interval <minutes_int>
    set emergency-interval <minutes_int>
    set alert-interval <minutes_int>
    set critical-interval <minutes_int>
    set error-interval <minutes_int>
    set warning-interval <minutes_int>
    set notification-interval <minutes_int>
    set information-interval <minutes_int>
    set debug-interval <minutes_int>
    set severity {alert | critical | debug | emergency | error
        | information | notification | warning}
    set IPS-logs {disable | enable}
    set firewall-authentication-failure-logs {disable | enable}
    set HA-logs {enable | disable}
    set IPsec-error-logs {disable | enable}
    set FDS-update-logs {disable | enable}
    set PPP-errors-logs {disable | enable}
    set sslvpn-authentication-errors-logs {disable | enable}
    set antivirus-logs {disable | enable}
    set webfilter-logs {disable | enable}
    set configuration-changes-logs {disable | enable}
    set violation-traffic-logs {disable | enable}
    set admin-login-logs {disable | enable}
    set local-disk-usage-warning {disable | enable}
    set FDS-license-expiring-warning {disable | enable}
    set FDS-license-expiring-days <days_int>
    set local-disk-usage <percentage>
    set fortiguard-log-quota-warning {disable | enable}
end
```


| Variable | Description | Default |
|------------------------------------|---|-------------|
| username <user-name_str> | Enter a valid email address in the format <code>user@domain.com</code> . This address appears in the From header of the alert email. | No default. |
| mailto1 <email-address_str> | Enter an email address. This is one of the email addresses where the FortiGate unit sends an alert email. | No default. |
| mailto2 <email-address_str> | Enter an email address. This is one of the email addresses where the FortiGate unit sends an alert email. | No default. |
| mailto3 <email-address_str> | Enter an email address. This is one of the email addresses where the FortiGate unit sends an alert email. | No default. |
| filter-mode {category threshold} | Select the filter mode of the alert email. The following fields display only when <code>threshold</code> is selected: <code>emergency-interval</code> <code>alert-interval</code> <code>critical-interval</code> <code>error-interval</code> <code>warning-interval</code> <code>notification-interval</code> <code>information-interval</code> <code>debug-interval</code> <code>severity</code> | category |
| email-interval <minutes_int> | Enter the number of minutes the FortiGate unit should wait before sending out an alert email. This is not available when <code>filter-mode</code> is <code>threshold</code> . | 5 |
| emergency-interval <minutes_int> | Enter the number of minutes the FortiGate unit should wait before sending out alert email for emergency level messages. Only available when <code>filter-mode</code> is <code>threshold</code> . | 1 |
| alert-interval <minutes_int> | Enter the number of minutes the FortiGate unit should wait before sending out an alert email for alert level messages. Only available when <code>filter-mode</code> is <code>threshold</code> . | 2 |
| critical-interval <minutes_int> | Enter the number of minutes the FortiGate unit should wait before sending out an alert email for critical level messages. Only available when <code>filter-mode</code> is <code>threshold</code> . | 3 |
| error-interval <minutes_int> | Enter the number of minutes the FortiGate unit should wait before sending out an alert email for error level messages. Only available when <code>filter-mode</code> is <code>threshold</code> . | 5 |

| Variable | Description | Default |
|---|---|---------|
| warning-interval <minutes_int> | Enter the number of minutes the FortiGate unit should wait before sending out an alert email for warning level messages. Only available when <code>filter-mode</code> is <code>threshold</code> . | 10 |
| notification-interval <minutes_int> | Enter the number of minutes the FortiGate unit should wait before sending out an alert email for notification level messages. Only available when <code>filter-mode</code> is <code>threshold</code> . | 20 |
| information-interval <minutes_int> | Enter the number of minutes the FortiGate unit should wait before sending out an alert email for information level messages. Only available when <code>filter-mode</code> is <code>threshold</code> . | 30 |
| debug-interval <minutes_int> | Enter the number of minutes the FortiGate unit should wait before sending out an alert email for debug level messages. Only available when <code>filter-mode</code> is <code>threshold</code> . | 60 |
| severity {alert critical debug emergency error information notification warning } | <p>Select the logging severity level. This is only available when <code>filter-mode</code> is <code>threshold</code>. The FortiGate unit logs all messages at and above the logging severity level you select. For example, if you select <code>error</code>, the unit logs <code>error</code>, <code>critical</code>, <code>alert</code>, and <code>emergency</code> level messages.</p> <p><code>alert</code> – Immediate action is required.</p> <p><code>critical</code> – Functionality is affected.</p> <p><code>debug</code> – Information used for diagnosing or debugging the FortiGate unit.</p> <p><code>emergency</code> – The system is unusable.</p> <p><code>error</code> – An erroneous condition exists and functionality is probably affected.</p> <p><code>information</code> – General information about system operations</p> <p><code>notification</code> – Information about normal events.</p> <p><code>warning</code> – Functionality might be affected.</p> | alert |
| IPS-logs {disable enable } | Enable or disable IPS logs. | disable |
| firewall-authentication-failure-logs {disable enable } | Enable or disable firewall authentication failure logs. | disable |
| HA-logs {enable disable } | Enable or disable high availability (HA) logs. | disable |
| IPsec-error-logs {disable enable } | Enable or disable IPsec error logs | disable |
| FDS-update-logs {disable enable } | Enable or disable FDS update logs. | disable |
| PPP-errors-logs {disable enable } | Enable or disable PPP error logs. | disable |
| sslvpn-authentication-errors-logs {disable enable } | Enable or disable SSL VPN authentication error logs. | disable |
| antivirus-logs {disable enable } | Enable or disable antivirus logs. | disable |
| webfilter-logs {disable enable } | Enable or disable web filter logs. | disable |

| Variable | Description | Default |
|--|---|---------|
| configuration-changes-logs {disable enable} | Enable or disable configuration changes logs. | disable |
| violation-traffic-logs {disable enable} | Enable or disable traffic violation logs. | disable |
| admin-login-logs {disable enable} | Enable or disable admin login logs | disable |
| local-disk-usage-warning {disable enable} | Enable or disable local disk usage warning in percent. For example enter the number 15 for a warning when the local disk usage is at 15 percent. The number cannot be 0 or 100. | disable |
| FDS-license-expiring-warning {disable enable} | Enable or disable to receive an email notification of the expire date of the FDS license. | disable |
| FDS-license-expiring-days <days_int> | Enter the number of days to be notified by email when the FDS license expires. For example, if you want notification five days in advance, enter 5. | 15 |
| local-disk-usage <percentage> | Enter a number for when the local disk's usage exceeds that number. | 75 |
| fortiguard-log-quota-warning {disable enable} | Enable to receive an alert email when the FortiGuard Log & Analysis server reaches its quota. | disable |

antivirus

Use antivirus commands to configure antivirus scanning for services, quarantine options, and to enable or disable grayware and heuristic scanning.

This chapter describes the following commands:

[heuristic](#)

[mms-checksum](#)

[notification](#)

[profile](#)

[quarantine](#)

[service](#)

[settings](#)

heuristic

Use this command to configure heuristic scanning for viruses in binary files.

Syntax

```
config antivirus heuristic
  set mode {pass | block | disable}
end
```

| Variable | Description | Default |
|-------------------------------|--|---------|
| mode {pass block disable} | Enter <code>pass</code> to enable heuristic scanning but pass detected files to the recipient. Suspicious files are quarantined if quarantine is enabled. Enter <code>block</code> to enable heuristic scanning and block detected files. A replacement message is forwarded to the recipient. Blocked files are quarantined if quarantine is enabled. Enter <code>disable</code> to disable heuristic scanning. | disable |

mms-checksum

Use this command in FortiOS Carrier to create a list of attachment checksum values. Messages containing these attachments can be blocked by the MMS profile.

Syntax

```
config antivirus mms-checksum
  edit <entry_id>
    set comment <comment_str>
    config entries
      edit <entry_name>
        set checksum <checksum_value>
        set status {enable | disable}
      end
    end
  end
```

| Variable | Description | Default |
|---------------------------|--------------------------------------|---------|
| comment <comment_str> | Optionally, enter a comment. | |
| <entry_name> | Enter a name for the blockable item. | |
| checksum <checksum_value> | Enter the checksum value. | |
| status {enable disable} | Enable the entry. | enable |

notification

Use this command for FortiOS Carrier to configure the viruses that trigger notification messages.

A notification list must be added to the MMS profile to generate notification messages.

Syntax

```
config antivirus notification
  edit <list_id_int>
    set name <name_str>
    set comment <comment_str>
    config entries
      edit <virus_str>
        set prefix {enable | disable}
        set status {enable | disable}
      end
    end
  end
```

| Keywords and variables | Description | Default |
|---------------------------|--|-------------|
| <list_id_int> | Enter the ID number of the list to edit. Each notification list has a unique ID number. Enter <code>edit ?</code> to view all the lists with their ID numbers. | No default. |
| name <name_str> | Enter a name for the notification list. If the list is new, you must enter a name. You can also use this command to change the name of an existing notification list. | No default. |
| comment <comment_str> | Enter an optional comment for the notification list. You can also use this command to change the name of an existing notification list. | No default. |
| <virus_str> | Enter the virus pattern to edit an existing list entry, or enter a new virus pattern to create a new list entry. | No default. |
| prefix {enable disable} | Enable to match the virus pattern with the beginning of any virus name. Disable to match the virus pattern with all of any virus name. For example, a pattern of <code>BDoor.ACJ!tr.bdr</code> with the prefix setting disabled will have the FortiGate unit check for a virus with that exact name. With the prefix setting enabled, a prefix match entry for <code>BDoor</code> will generate a notification message for any of the dozens of virus variants starting with <code>BDoor</code> . | enable |
| status {enable disable} | If required, you can disable a notification entry without removing it from the list. The FortiGate unit will ignore the list entry. By default, all list entries are enabled as soon as you create them. | enable |

profile

Use this command to configure UTM antivirus profiles for firewall policies. Antivirus profiles configure how virus scanning is applied to sessions accepted by a firewall policy that includes the antivirus profile.

Syntax

```
config antivirus profile
edit <name_str>
    set analytics-bl-filetype {1 | 2 | <filepattern_list_int>}
    set analytics-wl-filetype {1 | 2 | <filepattern_list_int>}
    set analytics-max-upload <mbytes>
    set av-virus-log {enable | disable}
    set av-block-log {enable | disable}
    set block-botnet-connections {enable | disable}
    set comment <comment_str>
    set extended-utm-log {enable | disable}
    set ftgd-analytics {disable | suspicious | everything}
    set inspection-mode {flow-based | proxy}
    config {http | https | ftp | ftps | imap | imaps | mapi | pop3 |
        pop3s | smb | smtp | smtps | nntp | im}
        set archive-block [corrupted encrypted mailbomb multipart
            nested unhandled]
        set archive-log [corrupted encrypted mailbomb multipart
            nested unhandled]
        set options {avmonitor | avquery | quarantine | scan}
    config nac-quar
        set infected {none | quar-interface | quar-scr-ip}
        set expiry <duration_str>
        set log {disable | enable}
    end
end
```

| Variable | Description | Default |
|--|---|---------|
| <name_str> | Enter the name of the antivirus profile. | |
| analytics-bl-filetype {1 2 <filepattern_list_int>} | Select file type pattern to blacklist and submit to FortiGuard Analytics: 1 — builtin patterns 2 — all executables <filepattern_list_int> — the identifier of a defined filepattern. See “ dlp filepattern ” on page 83. | 0 |
| analytics-wl-filetype {1 2 <filepattern_list_int>} | Select file type pattern to whitelist and not submit to FortiGuard Analytics: 1 — builtin patterns 2 — all executables <filepattern_list_int> — the identifier of a defined filepattern. See “ dlp filepattern ” on page 83. | 0 |

| Variable | Description | Default |
|--|---|---------|
| analytics-max-upload <mbytes> | Enter the maximum file size that can be scanned in Mbytes. Range: 1MB to 44MB | 10 |
| av-virus-log {enable disable} | Enable or disable logging for virus scanning. | disable |
| av-block-log {enable disable} | This command is no longer used. | disable |
| block-botnet-connections {enable disable} | Enable to block connections to known botnet servers. | disable |
| comment <comment_str> | Optionally enter a description of up to 63 characters of the antivirus profile. | |
| extended-utm-log {enable disable} | Enable or disable logging of UTM events. | disable |
| ftgd-analytics {disable suspicious everything} | FortiGuard Analytics mode: disable — FortiGuard Analytics disabled suspicious — send only suspicious items everything — send all items to FortiGuard | disable |
| inspection-mode {flow-based proxy} | Select flow-based or proxy antivirus protection. | proxy |

config {http | https | ftp | ftps | imap | imaps | mapi | pop3 | pop3s | smb | smtp | smtps | nntp | im}

Configure virus scanning options for the selected protocol.

| Variable | Description | Default |
|---|---|---------|
| archive-block [corrupted encrypted mailbomb multipart nested unhandled] | Select which types of archive to block. | null |
| archive-log [corrupted encrypted mailbomb multipart nested unhandled] | Select which types of archive to log. | null |
| options {avmonitor avquery quarantine scan} | Select one or more options apply to virus scanning for the protocol. To select more than one, enter the option names separated by a space. Some options are only available for some protocols. avmonitor — log detected viruses, but allow them through the firewall without modification. avquery — use the FortiGuard AV query service. quarantine — quarantine files that contain viruses. This feature is available for FortiGate units that contain a hard disk or are connected to a FortiAnalyzer unit. scan — Scan files transferred using this protocol for viruses. | |

config nac-quar

Configure NAC quarantine virus scanning options.

| Variable | Description | Default |
|--|--|---------|
| expiry <duration_str> | Set the duration of the quarantine in the days, hours, minutes format ###d##h##m. The minimum setting is 5 minutes. The maximum is 364d23h59m. This field is available when infected is not none. | 5m |
| infected { none quar-interface quar-src-ip } | Select to quarantine infected hosts to banned user list. none — no action is taken. quar-interface — quarantine all traffic on infected interface. quar-src-ip — quarantine all traffic from source IP. | none |
| log { disable enable } | Enable or disabling logging for NAC quarantine. | disable |

quarantine

Use this command to set file quarantine options. FortiGate units with a hard disk or a connection to a FortiAnalyzer unit can quarantine files. FortiGate features such as virus scanning can quarantine files.

Syntax

```
config antivirus quarantine
  set agelimit <hours_int>
  set destination {disk | FortiAnalyzer | NULL}
  set drop-blocked {ftp ftps http imap mm1 mm3 mm4 mm7 nntp pop3
    smtp}
  set drop-heuristic {ftp ftps http im imap mm1 mm3 mm4 mm7 nntp pop3
    smtp}
  set drop-infected {ftp ftps http im imap mapi mm1 mm3 mm4 mm7 nntp
    pop3 smtp}
  set drop-intercepted {ftp http imap mm1 mm3 mm4 mm7 pop3 smtp}
  set lowspace {drop-new | ovrw-old}
  set maxfilesize <MB_int>
  set quarantine-quota <MB_int>
  set store-blocked {ftp http imap mm1 mm3 mm4 mm7 nntp pop3 smtp}
  set store-heuristic {ftp http im imap mm1 mm3 mm4 mm7 nntp pop3
    smtp}
  set store-infected {ftp ftps http https im imap imaps mm1 mm3 mm4
    mm7 nntp pop3 pop3s smtp smtps}
  set store-intercepted {ftp http imap mm1 mm3 mm4 mm7 pop3 smtp}
end
```

| Variable | Description | Default |
|---|--|---------|
| agelimit <hours_int> | Specify how long files are kept in quarantine to a maximum of 479 hours. The age limit is used to formulate the value in the TTL column of the quarantined files list. When the limit is reached the TTL column displays EXP and the file is deleted (although a record is maintained in the quarantined files list). Entering an age limit of 0 (zero) means files are stored on disk indefinitely depending on low disk space action. This option appears when destination is not set to NULL. | 0 |
| destination {disk FortiAnalyzer NULL} | The destination for quarantined files: disk is the FortiGate unit internal hard disk, if present. FortiAnalyzer is a FortiAnalyzer unit the FortiGate unit is configured to use. NULL disables the quarantine. This command appears only if the FortiGate unit has an internal hard disk or is configured to use a FortiAnalyzer unit. | NULL |

| Variable | Description | Default |
|--|--|--|
| drop-blocked {ftp ftps http imap mm1 mm3 mm4 mm7 nntp pop3 smtp} | Do not quarantine blocked files found in traffic for the specified protocols. The files are deleted. MM1, MM3, MM4, and MM7 traffic types supported only in FortiOS Carrier. | imap nntp |
| drop-heuristic {ftp ftps http im imap mm1 mm3 mm4 mm7 nntp pop3 smtp} | Do not quarantine files found by heuristic scanning in traffic for the specified protocols. NNTP support for this field will be added in the future. MM1, MM3, MM4, and MM7 traffic types supported in FortiOS Carrier. | http im imap nntp pop3 smtp |
| drop-infected {ftp ftps http im imap mapi mm1 mm3 mm4 mm7 nntp pop3 smtp} | Do not quarantine virus infected files found in traffic for the specified protocols. NNTP support for this field will be added in the future. MM1, MM3, MM4, and MM7 traffic types supported in FortiOS Carrier. | im imap nntp |
| drop-intercepted {ftp http imap mm1 mm3 mm4 mm7 pop3 smtp} | For FortiOS Carrier, do not quarantine intercepted files found in traffic for the specified protocols. The files are deleted. | imap smtp pop3 http ftp mm1 mm3 mm4 mm7 |
| lowspace {drop-new ovrw-old} | Select the method for handling additional files when the FortiGate hard disk is running out of space. Enter <code>ovwr-old</code> to drop the oldest file (lowest TTL), or <code>drop-new</code> to drop new quarantine files. This option appears when <code>destination</code> is not set to NULL. | ovrw-old |
| maxfilesize <MB_int> | Specify, in MB, the maximum file size to quarantine. The FortiGate unit keeps any existing quarantined files over the limit. The FortiGate unit does not quarantine any new files larger than this value. The file size range is 0-499 MB. Enter 0 for unlimited file size. | 0 |
| quarantine-quota <MB_int> | Set the antivirus quarantine quota in MB, which is the amount of disk space to reserve for quarantining files. | 0 |
| store-blocked {ftp http imap mm1 mm3 mm4 mm7 nntp pop3 smtp} | Quarantine blocked files found in traffic for the specified protocols. NNTP support for this field will be added in the future. HTTP, FTP, MM1, MM3, MM4, and MM7 traffic types supported in FortiOS Carrier. | No default. |
| store-heuristic {ftp http im imap mm1 mm3 mm4 mm7 nntp pop3 smtp} | Quarantine files found by heuristic scanning in traffic for the specified protocols. NNTP support for this field will be added in the future. MM1, MM3, MM4, and MM7 traffic types supported in FortiOS Carrier. | No default. |

| Variable | Description | Default |
|--|---|--|
| store-infected {ftp ftps http https im imap imaps mm1 mm3 mm4 mm7 nntp pop3 pop3s smtp smtps} | Quarantine virus infected files found in traffic for the specified protocols. NNTP support for this field will be added in the future. MM1, MM3, MM4, and MM7 traffic types supported in FortiOS Carrier. | No default. |
| store-intercepted {ftp http imap mm1 mm3 mm4 mm7 pop3 smtp} | Quarantine intercepted FortiOS Carrier files found in traffic of the specified protocols. | imap smtp pop3 http ftp mm1 mm3 mm4 mm7 |

service

Use this command to configure how the FortiGate unit handles antivirus scanning of large files in HTTP, HTTPS, FTP, POP3, IMAP, and SMTP traffic.

Syntax

```
config antivirus service <service_str>
    set block-page-status-code <integer>
    set scan-bzip2 {enable | disable}
    set uncompnestlimit <depth_int>
    set uncompsizelimit <MB_int>
end
```

| Variable | Description | Default |
|----------------------------------|--|---------|
| <service_str> | The service being configured: HTTP, HTTPS, FTP, FTPS, IM, IMAP, NNTP, POP3, SMTP. | |
| block-page-status-code <integer> | Set a return code for HTTP replacement pages. This field is only for the HTTP service. | 200 |
| scan-bzip2 {enable disable} | Enable to allow the antivirus engine to scan the contents of bzip2 compressed files. Requires antivirus engine 1.90 for full functionality. Bzip2 scanning is <i>extremely</i> CPU intensive. Unless this feature is required, leave <code>scan-bzip2</code> disabled. | disable |
| uncompnestlimit <depth_int> | Set the maximum number of archives in depth the AV engine will scan with nested archives. The limit is from 2 to 100. The supported compression formats are arj, bzip2, cab, gzip, lha, lzh, msc, rar, tar, and zip. Bzip2 support is disabled by default. | 12 |
| uncompsizelimit <MB_int> | Set the maximum uncompressed file size that can be buffered to memory for virus scanning. Enter a value in megabytes between 1 and the maximum oversize threshold. Enter "?" to display the range for your FortiGate unit. Enter 0 for no limit (not recommended). | 10 |

settings

Use this command to select the default antivirus database and to enable or disable grayware detection as part of antivirus scanning.

Syntax

```
config antivirus settings
  set default-db {extended | extreme | normal}
  set grayware {enable | disable}
end
```

| Variable | Description | Default |
|--|---|---------|
| default-db {extended extreme normal} | <p>Select the default antivirus database to use for virus scanning. You can override the default database for specific protocols in the antivirus profile, see “antivirus profile” on page 64.</p> <p>extended select the extended virus database, which includes both In the Wild viruses and a large collection of zoo viruses that are no longer seen in recent virus studies. It is suitable for an enhanced security environment.</p> <p>extreme select the extreme virus database, which includes both In the Wild viruses and all available zoo viruses that are no longer seen in recent virus studies. It is suitable for an enhanced security environment.</p> <p>normal select the regular virus database, which includes In the Wild viruses and most commonly seen viruses on the network. For regular virus protection, it is sufficient to use this database.</p> | normal |
| grayware {enable disable} | Enable or disable grayware detection. Grayware includes adware, dial, downloader, hacker tool, keylogger, RAT and spyware. | disable |

application

Use these commands to configure application control.

custom

list

name

custom

Use this command to create custom application definitions.

Syntax

```
config application custom
  edit <signature_tag_str>
    set behavior <behave_str>
    set category <cat_int>
    set comment <comment_str>
    set protocol <protocol_str | All>
    set technology <technology_str>
    set vendor <vendor_int>
  end
```

The category field is required.

| Variable | Description | Default |
|----------------------------------|--|-------------|
| <signature_tag_str> | | |
| behavior <behave_str> | Select the application behavior filter to apply. Options include 2 — Botnet 3 — Evasive 5 —Excessive-Bandwidth All —all of the above | No default. |
| category <cat_int> | Enter the category integer to specify an application category, or enter All to include all categories. To determine the available application categories, enter <code>set category ?</code> . | 0 |
| comment <comment_str> | | |
| protocol <protocol_str All> | Specify the protocols that this application uses. Enter one or more protocol numbers separated by spaces, or All. For a list of protocol numbers, enter <code>set protocols ?</code> . | No default. |
| technology <technology_str> | Select the technologies involved in these applications. Enter one or more of the following technology numbers separated by spaces, or enter All. 0 — Network protocol 1 — Browser-based 2 — Client-server 4 — Peer-to-peer | No default. |
| vendor <vendor_int> | Enter the vendors to include. Enter one or more vendor numbers separated by spaces, or enter all. For a list of vendor numbers, enter <code>set vendor ?</code> . | No default. |

list

Use this command to create application control lists and configure the application options.

Syntax

```
config application list
edit <app_list_str>
  config entries
  edit <id_integer>
    set action {block | pass | reset}
    set application [<app1_int> <app2_int> ...]
    set behavior {0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8}
    set block-audio {enable | disable}
    set block-encrypt {enable | disable}
    set block-file {enable | disable}
    set block-im {enable | disable}
    set block-photo {enable | disable}
    set block-video {enable | disable}
    set category {<cat_int> | All}
    set comment <comment_string>
    set im-no-content-summary {enable | disable}
    set inspect-anyport {enable | disable}
    set log-packet {disable | enable}
    set protocols <protocols_str>
    set popularity {1 2 3 4 5}
    set session-ttl <ttl_int>
    set shaper <shaper_str>
    set shaper-reverse <shaper_str>
    set sub-category {<subcat_int> | all}
    set tags <tag_str>
    set technology <technology_Str>
    set vendor <vendor_int>
  end
end
set comment <comment_string>
set extended-utm-log {enable | disable}
set log {enable | disable}
set options [allow-dns allow-http allow-icmp allow-ssl]
set other-application-action {block | pass}
set other-application-log {enable | disable}
set p2p-black-list [bittorrent edonkey skype]
set unknown-application-action {block | pass}
set unknown-application-log {disable | enable}
end
```

| Variable | Description | Default |
|---|--|-------------|
| <app_list_str> | The name of the application control list. | No default. |
| <id_integer> | Enter the unique ID of the list entry you want to edit, or enter an unused ID to create a new one. | |
| action {block pass reset} | Enter the action the FortiGate unit will take with traffic from the application of the specified type. block will stop traffic from the specified application. pass will allow traffic from the specified application. reset will reset the network connection. | block |
| application [<app1_int> <app2_int> ...] | Enter one or more application integers to specify applications. Enter set application ? to list all application integers in the currently configured category. | all |
| behavior {0 1 2 3 4 5 6 7 8} | Select the application behavior filter to apply. Options include 0 — Other 1 — Reasonable 2 — Botnet 3 — Evasion 4 — Loss of productivity 5 — Excessive bandwidth 6 — Tunneling 7 — Reconnaissance 8 — Encrypted tunneling | |
| block-audio {enable disable} | Enable to block audio. This command is available only when application is set to AIM, ICQ, MSN, or Yahoo. | disable |
| block-encrypt {enable disable} | Enable to block encrypted IM sessions. This command is available only when application is set to AIM, ICQ, MSN, or Yahoo. | disable |
| block-file {enable disable} | Enable to block IM file transfers. This command is available only when application is set to AIM, ICQ, MSN, or Yahoo. | disable |
| block-im {enable disable} | Enable to block instant messages. This command is available only when application is set to AIM, ICQ, MSN, or Yahoo. | disable |
| block-photo {enable disable} | Enable to block IM photo sharing. This command is available only when application is set to AIM, ICQ, MSN, or Yahoo. | disable |
| block-video {enable disable} | Enable to block MSN video chat. This command is available only when application is set to MSN. | disable |

| Variable | Description | Default |
|---|---|-------------|
| category {<cat_int> All} | <p>Enter the category integer to specify an application category, or enter All to include all categories.</p> <p>Set a specific category to limit the scope of the All setting of the application command. For example, setting category to im and application to All will have the list entry include all IM applications. Similarly, the applications listed with the set application ? command will be limited to the currently configured category.</p> <p>Enter set category ? to list all category integers.</p> | All |
| comment <comment_string> | Optionally, enter a descriptive comment. | No default. |
| extended-utm-log {enable disable} | Enable or disable logging of UTM events. | disable |
| im-no-content-summary {enable disable} | <p>Enable to prevent display of content information on the dashboard.</p> <p>This command is available only when application is set to AIM, ICQ, MSN, or Yahoo.</p> | disable |
| inspect-anyport {enable disable} | <p>Enable to inspect all ports not used by any proxy for IM traffic.</p> <p>This command is available only when application is set to AIM, ICQ, MSN, or Yahoo.</p> | disable |
| log-packet {disable enable} | Enable or disable packet logging for an application in the application control list. | disable |
| log {enable disable} | Enable or disable logging. | disable |
| options [allow-dns allow-http allow-icmp allow-ssl] | Enable basic application signatures by default. | allow-dns |
| other-application-action {block pass} | Enter the action the FortiGate unit will take for unrecognized application traffic or supported application traffic not configured in the current application control list. | pass |
| other-application-log {enable disable} | Enter the logging action the FortiGate unit will take for unrecognized application traffic or supported application traffic not configured in the current application control list. | disable |
| p2p-black-list [bittorrent edonkey skype] | <p>P2P software tends to be evasive. Using this option you may be able to enhance P2P application detection by matching patterns found in P2P traffic detected in the last three minutes with new traffic to determine if the new traffic is P2P traffic.</p> <p>For example, if you set p2p-black-list to skype, the IPS looks for patterns in new traffic that match patterns in Skype traffic detected within the last three minutes. If a match is found the IPS assumes that this new traffic is also Skype traffic. Three minutes is how long information about matched P2P traffic remains in shared memory.</p> | null |
| popularity {1 2 3 4 5} | Enter the popularity levels of this application. | |

| Variable | Description | Default |
|--|--|-------------|
| protocols <protocols_str> | Enter the protocols that these applications use. Enter one or more protocol numbers separated by spaces. For a list of protocol numbers, enter <code>set protocols ?</code> . | No default. |
| session-ttl <ttl_int> | Enter the application's session TTL. Enter 0 to disable this option. If this option is not enabled, the TTL defaults to the setting of the <code>config system session-ttl</code> CLI command. | 0 |
| shaper <shaper_str> | Enter the name of a traffic shaper to enable traffic shaping for this application. | No default |
| shaper-reverse <shaper_str> | Enter the name of a traffic shaper to enable reverse traffic shaping for this application. | No default |
| sub-category {<subcat_int> all} | Enter the sub-category integer to specify an application sub-category, or enter <code>all</code> to include all sub-categories. To see a list of sub-category numbers, enter <code>set category ?</code> . | all |
| tags <tag_str> | Optionally, assign object tags. | No default. |
| technology <technology_Str> | Select the technologies involved in these applications. Enter one or more of the following technology numbers separated by spaces, or enter <code>all</code> . 0—Other 1—Web browser 2—Client 3—Server 4—Peer-to-peer | all |
| unknown-application-action {block pass} | Pass or block applications that have not been added to this application list. | pass |
| unknown-application-log {disable enable} | Enable or disable recording log messages when an application not added to the application list is detected. | disable |
| vendor <vendor_int> | Enter the vendors to include. Enter one or more vendor numbers separated by spaces, or enter <code>all</code> . For a list of vendor numbers, enter <code>set vendor ?</code> . | all |

name

Use this command to view the settings of each application. The application category and ID are displayed. This command is ‘read only’ and cannot be used to change application settings.

Syntax

```
config application name <app_str>
  get
end
```

| Variable | Description | Default |
|----------------|---|------------|
| name <app_str> | Enter the name of the application you want to view. Enter <code>config application name ?</code> to list all the applications. | No default |

client-reputation

Use these commands to configure client reputation tracking.

`profile`

profile

Use this command to configure client reputation profiles.

Syntax

```
config client-reputation profile
    set blocked-connection {disable | low | medium | high | critical}
    set failed-connection {disable | low | medium | high | critical}
    set malware-detected {disable | low | medium | high | critical}
    set max-rep-db-size <MBytes_int>
    set url-block-detected {disable | low | medium | high | critical}
    set window-size <wsize_int>
    config application
        edit <app_id>
            set category <category_int>
            set level {disable | low | medium | high | critical}
        end
    config geolocation
        edit <geoentry_ID>
            set country <country_code>
            set level {disable | low | medium | high | critical}
        end
    config ips
        set low <int>
        set medium <int>
        set high <int>
        set critical <int>
    end
    config level
        set low <int>
        set medium <int>
        set high <int>
        set critical <int>
    end
    config web
        edit <webentry_ID>
            set group <group_ID>
            set level {disable | low | medium | high | critical}
        end
    end
end
```

| Variable | Description | Default |
|---|---|---------|
| blocked-connection {disable low medium high critical} | Select which score level to use for blocked connection status: low, medium, high or critical. | high |
| failed-connection {disable low medium high critical} | Select which score level to use for failed connection status: low, medium, high or critical. | low |
| malware-detected {disable low medium high critical} | Select which score level to use for malware detected status: low, medium, high or critical. | low |

| Variable | Description | Default |
|---|---|-------------|
| max-rep-db-size <MBytes_int> | Set the maximum client reputation database size in MBytes. Range 10 to 2000. | 100 |
| url-block-detected {disable low medium high critical} | Select which score level to use for URL block detected status: low, medium, high or critical. | low |
| window-size <wsize_int> | Enter the reputation data window size. Range: 1 to 30 days. | 7 |
| config application variables | | |
| <app_id> | Enter an ID number for this application. | |
| category <category_int> | Enter the category. To view the list of categories, enter <code>set category ?</code> | No default. |
| level {disable low medium high critical} | Select which score level to use: disable, low, medium, high or critical. | low |
| config geolocation variables | | |
| <geentry_ID> | Enter an ID for this entry. | |
| country <country_code> | Enter the country code. For a list of country codes, enter <code>set country ?</code> | No default. |
| level {disable low medium high critical} | Select which score level to use: disable, low, medium, high or critical. | low |
| config ips variables | | |
| info-severity-status {enable disable} | Enable Information severity status level. | disable |
| low-severity-status {enable disable} | Enable Low severity status level. | disable |
| medium-severity-status {enable disable} | Enable Medium severity status level. | disable |
| high-severity-status {enable disable} | Enable High severity status level. | disable |
| critical-severity-status {enable disable} | Enable Critical severity status level. | disable |
| config level variables | | |
| low <int> | Set low threshold. Range 1 to 10. | 5 |
| medium <int> | Set medium threshold. Range 5 to 30. | 10 |
| high <int> | Set high threshold. Range 10 to 50. | 30 |
| critical <int> | Set critical threshold. Range 30 to 100. | 50 |
| config web variables | | |
| <webentry_ID> | Enter an ID for this entry. | |
| group <group_ID> | Enter the group category ID. For a list of ID values, enter <code>set group ?</code> | No default. |
| level {disable low medium high critical} | Select which score level to use: disable, low, medium, high or critical. | low |



Use these commands to configure Data Leak Prevention (DLP).

`filepattern`

`fp-doc-source`

`fp-sensitivity`

`sensor`

`settings`

filepattern

Use this command to add, edit or delete the file patterns used for DLP file blocking and to set which protocols to check for files to block.

Syntax

```
config dlp filepattern
  edit <filepattern_list_int>
    set name <list_name_str>
    set comment <comment_str>
  config entries
    edit <filepattern_str>
      set file-type {unknown | ignored | activemime | arj
        | aspack | base64 | bat | binhex | bzip | bzip2 | cab
        | jad | elf | exe | fsg | gzip | hlp | hta | html
        | javascript | lzh | msc | msoffice | mime | petite
        | prc | rar | class | sis | tar | upx | uue | cod
        | zip}
      set filter-type {pattern | type}
    end
  end
```

| Variable | Description | Default |
|---|--|---------|
| <filepattern_list_int> | A unique number to identify the file pattern list. | |
| name <list_name_str> | Enter a name for the file pattern header list. | |
| comment <comment_str> | Optionally enter a comment about the file pattern header list. | |
| <filepattern_str> | The name of the file pattern being configured. This can be any character string. | |
| file-type {unknown ignored activemime arj aspack base64 bat binhex bzip bzip2 cab jad elf exe fsg gzip hlp hta html javascript lzh msc msoffice mime petite prc rar class sis tar upx uue cod zip} | <p>This command is only available and valid when <code>filter-type</code> is set to <code>type</code>.</p> <p>Select the type of file the file filter will search for. Note that unlike the file pattern filter, this file type filter will examine the file contents to determine the what type of file it is. The file name and file extension is ignored.</p> <p>Because of the way the file type filter works, renaming files to make them appear to be of a different type will not allow them past the FortiGate unit without detection.</p> <p>Two of the available options are not file types:</p> <ul style="list-style-type: none"> Select <code>unknown</code> to configure a rule affecting every file format the file type filter unit does not recognize. Unknown includes every file format not available in the <code>file-type</code> command. Select <code>ignored</code> to configure a rule affecting traffic the FortiGate unit typically does not scan. This includes primarily streaming audio and video. | unknown |

| Variable | Description | Default |
|------------------------------|--|---------|
| filter-type {pattern type} | <p>Select the file filter detection method.</p> <ul style="list-style-type: none">• Enter <code>pattern</code> to examine files only by their names. For example, if <code>filter-type</code> is set to <code>pattern</code>, and the pattern is <code>*.zip</code>, all files ending in <code>.zip</code> will trigger this file filter. Even files ending in <code>.zip</code> that are not actually ZIP archives will trigger this filter.• Enter <code>type</code> to examine files only by their contents. Using the above example, if <code>filter-type</code> is set to <code>type</code>, and the type is <code>zip</code>, all ZIP archives will trigger this file filter. Even files renamed with non-zip file extensions will trigger this filter. | pattern |

fp-doc-source

Use this command to add fingerprinting document sources including the server and filepath for the source files.

Syntax

```
config dlp fp-doc-source
  edit <name>
    set date <int>
    set file-path <server_filepath>
    set file-pattern <wildcard_pattern>
    set keep-modified {enable | disable}
    set password <pwd_string>
    set period {daily | weekly | monthly | none}
    set remove-deleted {enable | disable}
    set scan-subdirectories {enable | disable}
    set sensitivity <name>
    set server <server_location>
    set server-type <samba>
    set tod-hour <int>
    set tod-min <int>
    set username <string>
    set vdom {mgmt | current}
    set weekday {day_str}
  end
```

| Variable | Description | Default |
|---|---|---------|
| <name> | Enter a name for this document source. | |
| date <int> | Set the date (day of month) to check the server. This is available when period is monthly. | 1 |
| file-path <server_filepath> | Enter the path to the file on the server. | |
| file-pattern <wildcard_pattern> | Enter the file pattern to match when using DLP blocking. Can include wildcards, and should include file type. For example to match all files that end in fortinet.xls you would enter <code>set file-pattern "*fortinet.xls"</code> | |
| keep-modified {enable disable} | Enable to keep modified files in the list. | |
| password <pwd_string> | Enter the Samba password string to use when logging into the server. | none |
| period {daily weekly monthly none} | Select the interval of time to use when checking the server. | |
| remove-deleted {enable disable} | Select enable to remove deleted chunks of documents from the server. | |
| scan-subdirectories {enable disable} | Enable to scan directories contained in the current directory while fingerprinting documents. | |
| sensitivity <name> | Select a configured sensitivity label to apply to this configuration. | |
| server <server_location> | Enter the IP address or IPv6 location of the server. | |

| Variable | Description | Default |
|-----------------------|--|---------|
| server-type <samba> | Enter the type of DLP server. Currently only samba servers are supported. | samba |
| tod-hour <int> | Set the time of day (hour) to check the server. This is available when <code>period</code> is not none. | 1 |
| tod-min <int> | Set the time of day (minute) to check the server. This is available when <code>period</code> is not none. | 0 |
| username <string> | Enter the Samba login name to use when logging into the server. | |
| vdom {mgmt current} | Choose whether to perform document fingerprinting from the current VDOM or the management VDOM. Through the management VDOM, files might be accessible that are not accessible via the current VDOM. | mgmt |
| weekday {day_str> | Enter the day of the week (e.g., "monday") to check the server. This is available when <code>period</code> is weekly. | sunday |

fp-sensitivity

Use this command to add fingerprinting sensitivity labels that can be applied to document sources and DLP rules.

These entries are labels only.

Syntax

```
config dlp fp-sensitivity
  edit <name_string>
end
```

| Variable | Description | Default |
|---------------|---|-------------|
| <name_string> | Enter a string that will be a label. It will be used to describe DLP rules. | No default. |

sensor

Use this command to create a DLP sensor.

Syntax

```
config dlp sensor
  edit <sensor_str>
    set comment <comment_str>
    set dlp-log {enable | disable}
    set extended-utm-log {enable | disable}
    set flow-based {enable | disable}
    set full-archive-proto {aim ftp http-get http-post icq imap mapi
      msn nntp pop3 smtp yahoo}
    set options {strict-file}
    set replacemsg-group <group_name>
    set summary-proto {aim ftp http-get http-post icq imap mapi msn
      nntp pop3 smtp yahoo}
  config filter
    edit <filter_str>
      set action {block | log-only | none | quarantine-ip }
      set expiry <duration_str>
      set filter-by {credit-card | encrypted | file-size | file-
        type | fingerprint | regexp | ssn | watermark}
      set proto {http-get http-post}
      set type {file | message}
    end
  end
end
```

| Variable | Description | Default |
|--|---|-------------|
| <sensor_str> | Enter the name of a sensor to edit. Enter a new name to create a new DLP sensor. | No default. |
| comment <comment_str> | Enter an optional description of the DLP sensor. Enclose the description in quotes if you want to include spaces. | No default. |
| dlp-log {enable disable} | Enable or disable logging for data leak prevention | enable |
| extended-utm-log {enable disable} | Enable or disable detailed UTM log messages. | disable |
| flow-based {enable disable} | Enable or disable flow-based DLP. | disable |
| full-archive-proto {aim ftp http-get http-post icq imap mapi msn nntp pop3 smtp yahoo} | Enter the protocols to always content archive. | null |
| options {strict-file} | strict-file is required for file filtering to function when the URL contains a ? character. For example, a file pattern configured to block *.exe will not block file.exe if the URL is www.example.com/download?filename=file.exe unless strict-file is specified. | No default |

| Variable | Description | Default |
|--|--|---|
| replacemsg-group <group_name> | Enter the replacement message group to use. | No default |
| summary-proto { aim ftp http-get http-post icq imap mapi msn nntp pop3 smtp yahoo } | Enter the protocols to always log summary. | aim ftp http-get http-post icq imap mapi msn nntp pop3 smtp yahoo |
| edit <filter_str> | Add a rule to a sensor by specifying the name of a DLP rule that has already been added. | No default |
| action { block log-only none quarantine-ip } | Enter the action taken when the rule is triggered. block — prevents the traffic matching the rule from being delivered. log-only — Prevent the DLP rule from taking any action on network traffic but log the rule match. Other matching rules in the same sensor and other sensors may still operate on matching traffic. none — Take no action. quarantine-ip — Block access through the FortiGate unit for any IP address that sends traffic matching a sensor with this action. The IP address is added to the Banned User list. | none |
| expiry <duration_str> | Set the duration of the quarantine in the days, hours, minutes format ###d##h##m. The minimum setting is 5 minutes. The maximum is 364d23h59m. This field is available when action is quarantine-ip. | 5m |
| filter-by { credit-card encrypted file-size file- type fingerprint regexp ssn watermark } | Select what the sensor filters by. | |
| proto { http-get http-post } | Enter the HTTP protocols to detect. Values are HTTP-GET and HTTP-PUT. | http-get http-post |
| type { file message } | | file |

settings

Use this command designate logical storage for DLP fingerprinting database.

These entries are labels only.

Syntax

```
config dlp settings
    set cache-mem-percent <memmax_int>
    set db-mode {remove-modified-then-oldest | remove-oldest | stop-adding}
    set size <maxsize_int>
    set storage-device <device>
end
```

| Variable | Description | Default |
|---|---|-------------|
| cache-mem-percent <memmax_int> | Enter the maximum portion of available memory allocated to caching. Range: 1 to 15 percent. | 2 |
| db-mode {remove-modified-then-oldest remove-oldest stop-adding} | Select the method of maintaining the database size. remove-modified-then-oldest — remove oldest chunks first, and then remove oldest file entries remove-oldest — just remove the oldest files first stop-adding — don't remove files, just stop adding to it. | stop-adding |
| size <maxsize_int> | Enter the maximum total size of files within storage in MB. | 16 |
| storage-device <device> | Enter the storage device name. | No default. |

endpoint-control

Use endpoint-control commands to configure the following parts of the Endpoint NAC feature:

- Endpoint license registration synchronization
- Endpoint NAC profiles
- the required minimum version of FortiClient Endpoint Security
- the FortiClient installer download location

Endpoint NAC is enabled in firewall policies.

This chapter contains the following sections:

[forticlient-registration-sync](#)

[profile](#)

[settings](#)

forticlient-registration-sync

Use this command to configure peer FortiGate units for synchronization of Endpoint license registration.



Units can synchronize registration data only if they are both running the same version of FortiOS with the same word size (32-bit or 64-bit).

Syntax

```
config endpoint-control forticlient-registration-sync
edit <peer-name>
    set peer-ip <addr_ipv4>
end
```

| Variable | Description | Default |
|---------------------|---|-------------|
| <peer-name> | Enter a name to identify the peer FortiGate unit. | No default. |
| peer-ip <addr_ipv4> | Enter the IP address of the peer FortiGate unit. | No default. |

profile

Use this command to configure an Endpoint NAC profile.

Syntax

```

config endpoint-control profile
  edit <profile_name>
    set description <string>
    set replacemsg-override-group <groupname_string>
    set device-groups <group_list>
    set users <user_list>
    set user-groups <usergroup_list>
  config forticlient-winmac-settings
    set forticlient-application-firewall {enable | disable}
    set forticlient-application-firewall-list <applist_name>
    set forticlient-ad {enable | disable}
    set forticlient-advanced-cfg {enable | disable}
    set forticlient-advanced-cfg-buffer <xml_config_str>
    set forticlient-advanced-vpn {enable | disable}
    set forticlient-advanced-vpn-buffer <xml_config_str>
    set forticlient-av {enable | disable}
    set forticlient-log-upload {enable | disable}
    set forticlient-log-upload-schedule {daily | hourly}
    set forticlient-log-upload-server {FQDN | ip4_addr}
    set forticlient-settings-lock {enable | disable}
    set forticlient-settings-lock-passwd <pwd_str>
    set forticlient-ui-options {af av vpn vs wf}
    set forticlient-update-from-fmg {enable | disable}
    set forticlient-update-server {<FQDN | ip4_addr>
      [<FQDN | ip4_addr> <FQDN | ip4_addr>]}
    set forticlient-vpn-provisioning {enable | disable}
    set view-profile-details {enable | disable}
  config forticlient-vpn-settings
    edit <vpn_name>
      set remote-gw <ipv4_addr>
      set auth-method {certificate | psk}
      set preshared-key <psk_str>
      set ssl-require-certificate {enable | disable}
      set ssl-vpn-access-port <port_int>
      set type {ipsec | ssl}
    end
    set forticlient-vuln-scan {enable | disable}
    set forticlient-vuln-scan-schedule {daily | weekly | monthly}
    set forticlient-vuln-scan-on-registration {enable | disable}
    set forticlient-wf {enable | disable}
    set forticlient-wf-profile <profile_name>
    set disable-wf-when-protected {enable | disable}
  end
end

```

```

config forticlient-android-settings
    set forticlient-advanced-cfg {enable | disable}
    set forticlient-advanced-cfg-buffer <xml_config_str>
    set forticlient-advanced-vpn {enable | disable}
    set forticlient-advanced-vpn-buffer <xml_config_str>
    set forticlient-vpn-provisioning {enable | disable}
    config forticlient-vpn-settings
        edit <vpn_name>
            set remote-gw <ipv4_addr>
            set auth-method {certificate | psk}
            set preshared-key <psk_str>
            set ssl-require-certificate {enable | disable}
            set ssl-vpn-access-port <port_int>
            set type {ipsec | ssl}
        end
    set forticlient-wf {enable | disable}
    set disable-wf-when-protected {enable | disable}
end
config forticlient-ios-settings
    set client-vpn-provisioning {enable | disable}
    set forticlient-advanced-cfg {enable | disable}
    set forticlient-advanced-cfg-buffer <xml_config_str>
    set forticlient-advanced-vpn {enable | disable}
    set forticlient-advanced-vpn-buffer <xml_config_str>
    config client-vpn-settings
        edit <vpn_name>
            set type {ipsec | ssl}
            set vpn-configuration-name <cfg_name_str>
            set vpn-configuration-content <str>
            set remote-gw <addr>
            set sslvpn-access-port <port_int>
            set sslvpn-require-certificate {enable | disable}
        end
    set distribute-configuration-profile {enable | disable}
    set configuration-name <str>
    set configuration-content <str>
    set forticlient-wf {enable | disable}
    set disable-wf-when-protected {enable | disable}
end
end

```

| Variable | Description | Default |
|---|---|-------------|
| <profile_name> | Enter a name for this Endpoint NAC profile. | No default. |
| client-vpn-provisioning {enable disable} | Enable or disable setting client VPN configuration. This is available under config forticlient-ios-settings only. | disable |
| description <string> | Optionally, enter a description enclosed in quote (") marks. | No default. |

| Variable | Description | Default |
|---|---|-------------|
| device-groups <group_list> | Enter a space-delimited list of the device groups that are assigned to this endpoint profile. | null |
| forticlient-application-firewall {enable disable} | Enable application detection. | disable |
| forticlient-application-firewall-list <applist_name> | Enter the name of the application list to use. See application list . | No default. |
| forticlient-ad {enable disable} | Enable or disable FortiClient advertising. | disable |
| forticlient-advanced-cfg {enable disable} | Enable or disable setting a custom FortiClient configuration. | disable |
| forticlient-advanced-cfg-buffer <xml_config_str> | Custom FortiClient configuration in XML format, enclosed in quote (") marks. Available when forticlient-advanced-cfg is enabled. Maximum buffer size is 32KB. | No default. |
| forticlient-advanced-vpn {enable disable} | Enable or disable setting custom FortiClient VPN configuration. | disable |
| forticlient-advanced-vpn-buffer <xml_config_str> | Custom FortiClient VPN configuration in XML format, enclosed in quote (") marks. Available when forticlient-advanced-vpn is enabled. | No default. |
| forticlient-av {enable disable} | Enable or disable FortiClient antivirus protection. | disable |
| forticlient-log-upload {enable disable} | Enable or disable uploading logs to FortiAnalyzer unit via FortiGate unit. | disable |
| forticlient-log-upload-schedule {daily hourly} | Set log upload schedule. | hourly |
| forticlient-log-upload-server {FQDN ip4_addr} | Set upload forticlient log upload server. | null |
| forticlient-settings-lock {enable disable} | Enable to lock FortiClient settings. This is available if forticlient-config-deployment is enable. | disable |
| forticlient-settings-lock-passwd <pwd_str> | Set the password to unlock FortiClient configuration. This is available when forticlient-settings-lock is enable. | No default. |
| forticlient-ui-options {af av vpn vs wf} | Set the user interface components of FortiClient that will be available to the user. af - application firewall av - antivirus vpn - VPN vs - vulnerability scan wf - web filtering | av vpn wf |
| forticlient-update-from-fmg {enable disable} | Enable or disable FortiClient update from FortiManager. | disable |
| forticlient-update-server {<FQDN ip4_addr> [<FQDN ip4_addr> <FQDN ip4_addr>]} | Enter one or more FortiClient update servers. Separate entries with spaces. | null |
| forticlient-vpn-provisioning {enable disable} | Enable or disable setting FortiClient VPN configuration. | disable |

| Variable | Description | Default |
|--|---|-------------|
| forticlient-vuln-scan {enable disable} | Enable or disable endpoint vulnerability scanning. | disable |
| forticlient-vuln-scan-schedule {daily weekly monthly} | Set endpoint vulnerability scan schedule. | monthly |
| forticlient-vuln-scan-on-registration {enable disable} | Enable or disable endpoint vulnerability scan when endpoint registers. | enable |
| forticlient-wf {enable disable} | Enable or disable FortiClient web category filtering. | |
| forticlient-wf-profile <profile_name> | FortiClient web filter profile to use. | default |
| disable-wf-when-protected {enable disable} | Disable FortiClient webfiltering when FortiGate unit is providing web filtering. | enable |
| users <user_list> | Enter a space-separated list of the users to whom this profile applies. This is not available for the default profile. | No default. |
| user-groups <usergroup_list> | Enter a space-separated list of the user groups to which this profile applies. This is not available for the default profile. | No default. |
| view-profile-details {enable disable} | Enable or disable client viewing of profile settings. | enable |
| replacemsg-override-group <groupname_string> | Enter the replacement message group name to use for portal message generating. The group must have its group-type set to <code>ec</code> . Maximum of 35 characters long. If no group is specified, the default will take effect. If the group does not contain certain <code>ec</code> messages they will be loaded from the per-vdom or global settings. | No default. |
| distribute-configuration-profile {enable disable} | Enable to provide .mobileconfig information to all iOS clients. | disable |
| configuration-name <str> | Enter the iOS configuration name. | No default. |
| configuration-content <str> | Enter XML .mobileconfig file content. | No default. |
| config client-vpn-settings variables | | |
| edit <vpn_name> | | No default. |
| type {ipsec ssl} | Select IPsec or SSL VPN. | ipsec |
| vpn-configuration-name <cfg_name_str> | Enter the name of the VPN configuration. (IPsec) | No default. |
| vpn-configuration-content <str> | Enter XML .mobileconfig file content. | No default. |
| remote-gw <addr> | Enter gateway FQDN or IP address. (SSL VPN) | No default. |
| sslvpn-access-port <port_int> | For SSL VPN, enter port number to use. | 443 |
| sslvpn-require-certificate {enable disable} | For SSL VPN, enable or disable authenticating clients by certificate. | disable |
| config forticlient-vpn-settings variables | | |
| edit <vpn_name> | | No default. |
| remote-gw <ipv4_addr> | Enter gateway IP address. | No default. |

| Variable | Description | Default |
|---|--|-------------|
| auth-method {certificate psk} | Select certificate or pre-shared key authentication. | psk |
| preshared-key <psk_str> | Enter the pre-shared key. | No default. |
| ssl-vpn-access-port <port_int> | For SSL VPN, enter port number to use. | 443 |
| ssl-require-certificate {enable disable} | For SSL VPN, enable or disable authenticating clients by certificate. | disable |
| type {ipsec ssl} | Select IPsec or SSL VPN. | ipsec |

settings

Use this command to configure the FortiClient Endpoint Security installer download location. This is part of the Endpoint Control feature.

Syntax

```
config endpoint-control settings
    set download-location {custom | fortigate | fortiguard}
    set download-custom-link <url>
    set forticlient-keepalive-interval <secs_int>
    set forticlient-reg-key-enforce {enable | disable}
    set forticlient-reg-key <key_str>
    set forticlient-reg-timeout <days_int>
    set forticlient-sys-update-interval <upd_int>
end
```

| Variable | Description | Default |
|---|--|-------------|
| download-location {custom fortigate fortiguard} | Select location from which FortiClient application is downloaded: custom — set download-custom-link to a URL that provides the download fortigate — this FortiGate unit, available on some models fortiguard — FortiGuard Services | fortiguard |
| download-custom-link <url> | Enter a URL where the FortiClient installer can be downloaded. This is available if download-location is custom. | No default. |
| forticlient-keepalive-interval <secs_int> | Set the interval in seconds between FortiClient keep-alive messages. Range 20-86 400. | 120 |
| forticlient-reg-key-enforce {enable disable} | Enable enforcement of FortiClient registration key. | disable |
| forticlient-reg-key <key_str> | Enter the FortiClient registration key. | No default. |
| forticlient-reg-timeout <days_int> | Set the FortiClient license timeout in days. Range 1-180. | 7 |
| forticlient-sys-update-interval <upd_int> | Set the interval in minutes between system update messages from FortiClient. Range 30-1440. | 720 |
| version <major.minor.patch> | Enter the minimum acceptable version of the FortiClient application. This is available if version-check is minimum. | 4.0.0 |
| version-check {latest minimum} | Enter latest to require the newest version available from the download location. Enter minimum to specify a minimum version in version. This is available if enforce-minimum-version is enabled. | minimum |

firewall

Use firewall commands to configure firewall policies and the data they use.

This chapter contains the following sections:

| | | |
|--|---|---|
| address, address6 | ldb-monitor | shaper per-ip-shaper |
| addrgrp, addrgrp6 | local-in-policy, local-in-policy6 | shaper traffic-shaper |
| auth-portal | mms-profile | sniffer |
| carrier-endpoint-bwl | multicast-address | sniff-interface-policy |
| carrier-endpoint-ip-filter | multicast-policy | sniff-interface-policy6 |
| central-nat | policy, policy6 | ssl setting |
| deep-inspection-options | policy46, policy64 | ttl-policy |
| dnstranslation | profile-group | vip |
| DoS-policy, DoS-policy6 | profile-protocol-options | vip46 |
| gtp | schedule onetime | vip6 |
| identity-based-route | schedule recurring | vip64 |
| interface-policy | schedule group | vip64 |
| interface-policy6 | service category | |
| ipmacbinding setting | service custom | |
| ipmacbinding table | service group | |
| ippool, ippool6 | | |
| ip-translation | | |
| ipv6-eh-filter | | |

address, address6

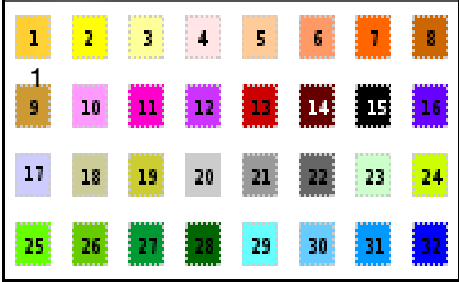
Use this command to configure firewall addresses used in firewall policies. An IPv4 firewall address is a set of one or more IP addresses, represented as a domain name, an IP address and a subnet mask, or an IP address range. An IPv6 firewall address is an IPv6 6-to-4 address prefix.

Addresses, address groups, and virtual IPs must have unique names to avoid confusion in firewall policies. If an address is selected in a policy, it cannot be deleted until it is deselected from the policy.

Syntax

```
config firewall address
    edit <name_str>
        set associated-interface <interface_str>
        set cache-ttl <ttl_int>
        set color <color_int>
        set comment <comment_string>
        set country <country_code>
        set end-ip <address_ipv4>
        set fqdn <domainname_str>
        set start-ip <address_ipv4>
        set subnet <address_ipv4mask>
        set tags <tags_str>
        set type {ipmask | iprange | fqdn | geography | network-service
                | wildcard}
        set visibility {enable | disable}
        set wildcard <address_ip4mask>
    config service
        edit <service_id>
            set end-port <port_int>
            set protocol {sctp | tcp | udp}
            set start-port <port_int>
        end
    end
end
config firewall address6
    edit <name_str>
        set ip6 <address_ipv6prefix>
    end
```

| Variable | Description | Default |
|---|---|-------------|
| The following fields are for config firewall address. | | |
| <name_str> | Enter the name of the address. | No default. |
| associated-interface <interface_str> | Enter the name of the associated interface. If not configured, the firewall address is bound to an interface during firewall policy configuration. | No default. |
| cache-ttl <ttl_int> | Enter minimum time-to-live (TTL) of individual IP addresses in FQDN cache. This is available when type is fqdn. | 0 |

| Variable | Description | Default |
|---|---|--------------------|
| color <color_int> | <p>Set the icon color to use in the web-based manager.</p> <p>0 sets the default, color 1.</p>  | 0 |
| comment <comment_string> | Enter a descriptive comment for this address. | No default. |
| country <country_code> | Enter the two-letter country code. For a list of codes, enter <code>set country ?</code> . This is available when <code>type</code> is <code>geography</code> . | null |
| end-ip <address_ipv4> | If <code>type</code> is <code>iprange</code> , enter the last IP address in the range. | 0.0.0.0 |
| fqdn <domainname_str> | If <code>type</code> is <code>fqdn</code> , enter the fully qualified domain name (FQDN). | No default. |
| start-ip <address_ipv4> | If <code>type</code> is <code>iprange</code> , enter the first IP address in the range. | 0.0.0.0 |
| subnet <address_ipv4mask> | <p>If <code>type</code> is <code>ipmask</code>, enter an IP address then its subnet mask, in dotted decimal format and separated by a space, or in CIDR format with no separation. For example, you could enter either:</p> <ul style="list-style-type: none"> 172.168.2.5/32 172.168.2.5 255.255.255.255 <p>The IP address can be for a single computer or a subnetwork. The subnet mask corresponds to the class of the IP address being added.</p> <ul style="list-style-type: none"> A single computer's subnet mask is 255.255.255.255 or /32. A class A subnet mask is 255.0.0.0 or /8. A class B subnet mask is 255.255.0.0 or /26. A class C subnet mask is 255.255.255.0 or /24. | 0.0.0.0 0.0.0.0 |
| tags <tags_str> | Enter object tags applied to this address. Separate tag names with spaces. | null |
| type {ipmask iprange fqdn geography network-service wildcard} | Select whether this firewall address is a subnet address, an address range, fully qualified domain name, a geography-based address, a network service or an IP with a wildcard netmask. | ipmask |
| visibility {enable disable} | Select whether this address is available in firewall policy address fields in the web-based manager. | enable |
| wildcard <address_ip4mask> | This is available if <code>type</code> is <code>wildcard</code> . | 0.0.0.0 0.0.0.0 |
| Fields for config service. type must be network-service | | |

| Variable | Description | Default |
|--|---|-------------|
| <service_id> | Enter an ID number, or 0 to auto-assign one. | |
| end-port <port_int> | Enter the last port in the service range. | 0 |
| protocol {sctp tcp udp} | Select the service protocol. | tcp |
| start-port <port_int> | Enter the first port in the service range. | 0 |
| The following fields are for config firewall address6. | | |
| <name_str> | Enter the name of the IPv6 address prefix. | No default. |
| ip6 <address_ipv6prefix> | If the IP address is IPv6, enter an IPv6 IP address prefix. | ::/0 |

addrgrp, addrgrp6

Use this command to configure firewall address groups used in firewall policies.

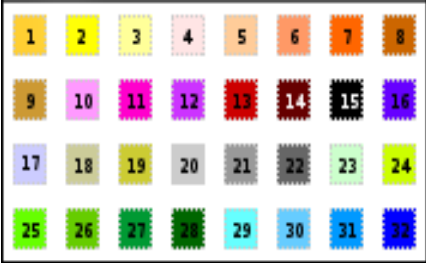
You can organize related firewall addresses into firewall address groups to simplify firewall policy configuration. For example, rather than creating three separate firewall policies for three firewall addresses, you could create a firewall address group consisting of the three firewall addresses, then create one firewall policy using that firewall address group.

Addresses, address groups, and virtual IPs must all have unique names to avoid confusion in firewall policies. If an address group is selected in a policy, it cannot be deleted unless it is first deselected in the policy.

An address group can be a member of another address group.

Syntax

```
config firewall addrgrp, addrgrp6
  edit <name_str>
    set comment <comment_string>
    set member <name_str>
    set visibility {enable | disable}
    set color <color_int>
  end
```

| Variable | Description | Default |
|------------------------------------|---|-------------|
| <name_str> | Enter the name of the address group. | No default. |
| comment <comment_string> | Enter any comments for this address group. | No default. |
| member <name_str> | Enter one or more names of firewall addresses to add to the address group. Separate multiple names with a space. To remove an address name from the group, retype the entire new list, omitting the address name. | No default. |
| visibility { enable disable } | Select whether this address group is available in firewall policy address group fields in the web-based manager. | enable |
| color <color_int> | Set the icon color to use in the web-based manager. 0 sets the default, color 1.  | 0 |

auth-portal

Use this command to add an external authentication portal.

Syntax

```
config firewall auth-portal
  set groups <group_list>
  set identity-based-route <route_name>
  set portal-addr <IP4_addr | FQDN>
  set portal-addr6 <IP6_addr | FQDN>
end
```

| Variable | Decription | Default |
|---|---|-------------|
| groups <group_list> | Enter the firewall user groups permitted to authenticate through this portal. Separate group names with spaces. | No default. |
| identity-based-route <route_name> | Enter the identity-based route that applies to this portal. | No default. |
| portal-addr <IP4_addr FQDN> portal-addr6 <IP6_addr FQDN> | Enter the IP address or FQDN of the authentication portal. Use portal-addr6 for IPv6 address. | No default. |

carrier-endpoint-bwl

Use FortiOS Carrier carrier end point filtering (also called carrier end point blocking) to control access to MMS services for users according to their carrier end point. Carrier end point filtering can filter MM1, MM3, MM4, and MM7 messages according to the carrier end points in the *From* or *To* addresses of the messages.

Syntax

```
config firewall carrier-endpoint-bwl
  edit <carr-endpnt-1st-integer>
    set comment <carr_endpnt_1st_comment>
    config entries
      edit <carr_endpnt_pattern>
        set pattern-type {regex | wildcard | simple}
        set action {none | block | exempt-mass-MMS | exempt }
        set log-action {archive | intercept}
        set status {enable | disable}
      next
    set name <carr_endpnt_1st_name>
  next
end
```

| Variable | Description | Default |
|---|---|-------------|
| action {none block exempt-mass-MMS exempt } | <p>The action (or actions archive and intercept) to take if the carrier end point expression is found in the list.</p> <p>none — no action is taken</p> <p>block — message is not delivered to intended recipient, log message in AV LOG as blocked due to carrier end point</p> <p>exempt-mass-MMS — no mass MMS scanning performed</p> <p>exempt — exempt user messages from all scanning</p> | block |
| log-action {archive intercept} | <p>archive — Message is delivered to intended recipient, MMS transaction is forwarded to FortiAnalyzer archive, an entry is generated in content summary for FortiGate unit.</p> <p>intercept — Message is delivered to intended recipient, files are quarantined based on quarantine configuration, log message in AV LOG as intercepted due to carrier end point.</p> | No default. |
| <carr_endpnt_1st_comment> | Optional description of the carrier end point filter list. The comment text must be less than 63 characters long, or it will be truncated. Spaces are replaced with a plus sign (+). | null |
| <carr_endpnt_pattern> | The carrier end point pattern to use for filtering/searching. | No default. |
| <carr-endpnt-1st-integer> | A unique number to identify the carrier end point filter list. | No default. |

| Variable | Description | Default |
|---|--|----------|
| name <carr_endpnt_lst_name> | The name of the carrier end point filter list. | null |
| pattern-type {regex wildcard simple} | Set the pattern type for the banned word. Choose from <code>regex</code> , <code>wildcard</code> ., or <code>simple</code> . Create patterns for banned carrier end point expressions using Perl regular expressions or wildcards. | wildcard |
| status {enable disable} | Enable carrier end point filter search for carrier end point expression in <code>carr-endpnt-expression</code> . | disable |

carrier-endpoint-ip-filter

In mobile networks, neither the user name nor the IP address can be used to identify a specific user. The only element unique to a user is the carrier end point. The carrier end point IP filter provides a mechanism to block network access for a specific list of carrier end points.

The carrier end point IP filter feature uses a carrier end point filter list created using the CLI command `config firewall carrier-endpoint-bwl`. To set up a carrier end point IP filter, you must create the carrier end point filter list prior to enabling the carrier end point IP filter feature.

Syntax

```
config firewall carrier-endpoint-ip-filter
edit <carr_endpnt>
    set log-status {enable | disable}
    set status {enable | disable}
next
end
```

| Variable | Description | Default |
|-------------------------------|--|------------|
| <carr_endpnt> | The carrier end point to be blocked. | No default |
| log-status {enable disable} | Enable or disable writing a log message when the carrier end point is blocked. | disable |
| status {enable disable} | Enable or disable blocking the carrier end point. | disable |

central-nat

Use this command to create NAT rules as well as NAT mappings that are set up by the global firewall table. Multiple NAT rules can be added on a FortiGate and these NAT rules can be used in firewall policies.

A Typical NAT rule consists of:

- source ip address
- original port number
- translated ip address
- translated port number

IP addresses can be single address or multiple addresses that are predefined with an IP pool. Similarly, port numbers can also be a single port or a range of ports.

Syntax

```
config firewall central-nat
  edit <name_str>
    set status {enable | disable}
    set orig-addr <name_ip>
    set nat-ippool <name_ip>
    set orig-port <port_int>
    set nat-port <port_int-port_int>
  end
end
```

| Variable | Description | Default |
|------------------------------|--|---------|
| status {enable disable} | Enable or disable central NAT rule | enable |
| orig-addr <name_ip> | Enter source ip address name | |
| nat-ippool <name_ip> | Enter translated ip pool name for translated addresses | |
| orig-port <port_int> | Enter port number of the source ip | 0 |
| nat-port <port_int-port_int> | Enter translated port or port range | 0 |

deep-inspection-options

Use this command to configure UTM deep inspection options profiles for firewall policies. Deep inspection options configure how UTM functionality identifies secure content protocols such as HTTPS, FTPS, and SMTPS. Client comforting options are controlled by the corresponding non-secure protocol options in [firewall profile-protocol-options](#).

To configure the ssl-server, change client-cert-request from bypass.

Syntax

```
config firewall deep-inspection-options
  edit <name_str>
    set caname <ca-cert_name>
    set certname <cert_name>
    set comment <comment_str>
    set extended-utm-log {enable | disable}
    set ssl-invalid-server-cert-log {enable | disable}
  config ftps
    set ports <port_number_list>
    set allow-invalid-server-cert {enable | disable}
    set client-cert-request {bypass | inspect | block}
    set ssl-ca-list {enable | disable}
    set status {enable | disable}
    set unsupported-ssl {bypass | block}
  end
  config https
    set ports <port_number_list>
    set allow-invalid-server-cert {enable | disable}
    set client-cert-request {bypass | inspect | block}
    set ssl-ca-list {enable | disable}
    set status {enable | disable}
    set unsupported-ssl {bypass | block}
  end
  config imaps
    set ports <port_number_list>
    set allow-invalid-server-cert {enable | disable}
    set client-cert-request {bypass | inspect | block}
    set ssl-ca-list {enable | disable}
    set status {enable | disable}
    set unsupported-ssl {bypass | block}
  end
  config pop3s
    set ports <port_number_list>
    set allow-invalid-server-cert {enable | disable}
    set client-cert-request {bypass | inspect | block}
    set ssl-ca-list {enable | disable}
    set status {enable | disable}
    set unsupported-ssl {bypass | block}
  end
end
```

```

config smtps
    set ports <port_number_list>
    set allow-invalid-server-cert {enable | disable}
    set client-cert-request {bypass | inspect | block}
    set ssl-ca-list {enable | disable}
    set status {enable | disable}
    set unsupported-ssl {bypass | block}
end
config ssl
    set allow-invalid-server-cert {enable | disable}
    set inspect-all {enable | disable}
    set ssl-ca-list {enable | disable}
end
config ssl-server
    edit <table_id>
        set ftps-client-cert-request {block | bypass | inspect}
        set https-client-cert-request {block | bypass | inspect}
        set imaps-client-cert-request {block | bypass | inspect}
        set ip <ipv4_addr>
        set pops3-client-cert-request {block | bypass | inspect}
        set smtps-client-cert-request {block | bypass | inspect}
        set ssl-other-client {block | bypass | inspect}
    end
end

```

| Variable | Description | Default |
|--|--|----------------------|
| <name_str> | Enter the name of the protocol options profile. | |
| caname <ca-cert_name> | Select the CA certificate used by SSL content scanning and inspection for establishing encrypted SSL sessions. | Fortinet_CA_SSLProxy |
| certname <cert_name> | Select the server certificate used by SSL inspection. | |
| comment <comment_str> | Optionally enter a description of up to 63 characters of the protocol options profile. | |
| extended-utm-log {enable disable} | Enable or disable detailed UTM log messages. | disable |
| ssl-invalid-server-cert-log {enable disable} | Enable or disable logging for SSL server certificate validation. extended-utm-log must be enabled. | disable |

config ftps

Configure FTPS protocol options.

| Variable | Description | Default |
|--|--|---------|
| ports <port_number_list> | Enter the port numbers to scan for FTPS content. | 990 |
| allow-invalid-server-cert {enable disable} | Enable to allow SSL sessions whose server certificate validation failed. | disable |

| Variable | Description | Default |
|---|---|---------|
| client-cert-request {bypass inspect block} | Select what action is taken by the FortiGate SSL proxy when the client certificate request fails during the SSL handshake. SSL sessions that use client-certificates bypass the SSL inspection by default. This command offers the options to inspect or block that traffic. | bypass |
| ssl-ca-list {enable disable} | Enable to verify SSL session server certificate against stored CA certificate list. | disable |
| status {enable disable} | Enable or disable FTPS protocol inspection. | enable |
| unsupported-ssl {bypass block} | Select whether to bypass or block undecryptable SSL sessions. | bypass |

config https

Configure HTTPS protocol options.

| Variable | Description | Default |
|---|---|---------|
| ports <port_number_list> | Enter the port numbers to scan for HTTPS content. | 443 |
| allow-invalid-server-cert {enable disable} | Enable to allow SSL sessions even if server certificate validation failed for the session. | disable |
| client-cert-request {bypass inspect block} | Select what action is taken by the FortiGate SSL proxy when the client certificate request fails during the SSL handshake. SSL sessions that use client-certificates bypass the SSL inspection by default. This command offers the options to inspect or block that traffic. | bypass |
| ssl-ca-list {enable disable} | Enable to verify SSL session server certificate against stored CA certificate list. | disable |
| status {enable disable} | Enable or disable HTTPS protocol inspection. | enable |
| unsupported-ssl {bypass block} | Select whether to bypass or block undecryptable SSL sessions. | bypass |

config imap

Configure secure IMAP (IMAPS) protocol options.

| Variable | Description | Default |
|---|---|---------|
| ports <port_number_list> | Enter the port numbers to scan for IMAPS content. | 993 |
| allow-invalid-server-cert {enable disable} | Enable to allow SSL sessions even if server certificate validation failed for the session. | disable |
| client-cert-request {bypass inspect block} | Select what action is taken by the FortiGate SSL proxy when the client certificate request fails during the SSL handshake. SSL sessions that use client-certificates bypass the SSL inspection by default. This command offers the options to inspect or block that traffic. | bypass |
| ssl-ca-list {enable disable} | Enable to verify SSL session server certificate against stored CA certificate list. | disable |

| Variable | Description | Default |
|---------------------------------------|---|---------|
| status { enable disable } | Enable or disable IMAPS protocol inspection. | enable |
| unsupported-ssl { bypass block } | Select whether to bypass or block undecryptable SSL sessions. | bypass |

config pop3s

Configure secure POP3 (POP3S) protocol options.

| Variable | Description | Default |
|---|---|---------|
| ports <port_number_list> | Enter the port numbers to scan for POP3S content. | 995 |
| allow-invalid-server-cert { enable disable } | Enable to allow SSL sessions even if server certificate validation failed for the session. | disable |
| client-cert-request { bypass inspect block } | Select what action is taken by the FortiGate SSL proxy when the client certificate request fails during the SSL handshake. SSL sessions that use client-certificates bypass the SSL inspection by default. This command offers the options to inspect or block that traffic. | bypass |
| ssl-ca-list { enable disable } | Enable to verify SSL session server certificate against stored CA certificate list. | disable |
| status { enable disable } | Enable or disable POP3S protocol inspection. | enable |
| unsupported-ssl { bypass block } | Select whether to bypass or block undecryptable SSL sessions. | bypass |

config smtps

Configure secure SMTP (SMTPS) protocol options.

| Variable | Description | Default |
|---|---|---------|
| ports <port_number_list> | Enter the port numbers to scan for SMTPS content. | 465 |
| allow-invalid-server-cert { enable disable } | Enable to allow SSL sessions even if server certificate validation failed for the session. | disable |
| client-cert-request { bypass inspect block } | Select what action is taken by the FortiGate SSL proxy when the client certificate request fails during the SSL handshake. SSL sessions that use client-certificates bypass the SSL inspection by default. This command offers the options to inspect or block that traffic. | bypass |
| ssl-ca-list { enable disable } | Enable to verify SSL session server certificate against stored CA certificate list. | disable |
| status { enable disable } | Enable or disable SMTPS protocol inspection. | enable |
| unsupported-ssl { bypass block } | Select whether to bypass or block undecryptable SSL sessions. | bypass |

config ssl

Configure SSL settings.

| Variable | Description | Default |
|---|--|---------|
| allow-invalid-server-cert {enable disable} | Enable to allow SSL sessions even if server certificate validation failed for the session. | disable |
| inspect-all {enable disable} | Inspect all. | disable |
| ssl-ca-list {enable disable} | Enable to verify SSL session server certificate against stored CA certificate list. | disable |

config ssl-server

Configure ssl server settings for use with the secure protocols (https, ftps, pop3s, smtps).

| Variable | Description | Default |
|---|--|---------|
| edit <table_id> | Enter a number to identify this SSL server in the list of configured SSL servers | |
| ftps-client-cert-request {block bypass inspect} | Select what action is taken by the FortiGate SSL proxy when the client certificate request fails during the FTPS client handshake. SSL sessions that use client-certificates bypass the SSL inspection by default. This command offers the options to inspect or block that traffic. | bypass |
| https-client-cert-request {block bypass inspect} | Select what action is taken by the FortiGate SSL proxy when the client certificate request fails during the HTTPS client handshake. SSL sessions that use client-certificates bypass the SSL inspection by default. This command offers the options to inspect or block that traffic. | bypass |
| imaps-client-cert-request {block bypass inspect} | Select what action is taken by the FortiGate SSL proxy when the client certificate request fails during the IMAPS client handshake. SSL sessions that use client-certificates bypass the SSL inspection by default. This command offers the options to inspect or block that traffic. | bypass |
| ip <ipv4_addr> | Enter the IP address of the SSL server. | |
| pops3-client-cert-request {block bypass inspect} | Select what action is taken by the FortiGate SSL proxy when the client certificate request fails during the POP3S client handshake. SSL sessions that use client-certificates bypass the SSL inspection by default. This command offers the options to inspect or block that traffic. | bypass |

| Variable | Description | Default |
|---|--|---------|
| smtps-client-cert-request {block bypass inspect} | <p>Select what action is taken by the FortiGate SSL proxy when the client certificate request fails during the SMTPS client handshake.</p> <p>SSL sessions that use client-certificates bypass the SSL inspection by default. This command offers the options to inspect or block that traffic.</p> | bypass |
| ssl-other-client {block bypass inspect} | <p>Select what action is taken by the FortiGate SSL proxy when the client certificate request fails during the client handshake for SSL protocols other than those above.</p> <p>SSL sessions that use client-certificates bypass the SSL inspection by default. This command offers the options to inspect or block that traffic.</p> | bypass |

dnstranslation

Use this command to add, edit or delete a DNS translation entry. If DNS translation is configured, the FortiGate unit rewrites the payload of outbound DNS query replies from internal DNS servers, replacing the resolved names' internal network IP addresses with external network IP address equivalents, such as a virtual IP address on a FortiGate unit's external network interface. This allows external network hosts to use an internal network DNS server for domain name resolution of hosts located on the internal network.

Syntax

```
config firewall dnstranslation
  edit <index_int>
    set dst <destination_ipv4>
    set netmask <address_ipv4mask>
    set src <source_ipv4>
  end
```

| Variable | Description | Default |
|-------------------------------|--|-------------|
| <index_int> | Enter the unique ID number of the DNS translation entry. | No default. |
| dst <destination_ipv4> | Enter the IP address or subnet on the external network to substitute for the resolved address in DNS query replies. dst can be either a single IP address or a subnet on the external network, but must be equal in number to the number of mapped IP addresses in src. | 0.0.0.0 |
| netmask <address_ipv4mask> | If src and dst are subnets rather than single IP addresses, enter the netmask for both src and dst. | 0.0.0.0 |
| src <source_ipv4> | Enter the IP address or subnet on the internal network to compare with the resolved address in DNS query replies. If the resolved address matches, the resolved address is substituted with dst. | 0.0.0.0 |

DoS-policy, DoS-policy6

Use these commands to configure Denial of Service (DoS) policies: `Dos-policy` applies to IPv4 traffic, `Dos-policy6` applies to IPv6 traffic.

FortiGate Intrusion Protection uses Denial of Service (DoS) sensors to identify network traffic anomalies that do not fit known or preset traffic patterns. Four statistical anomaly types for the TCP, UDP, and ICMP protocols can be identified.

| | |
|----------------------------------|---|
| Flooding | If the number of sessions targeting a single destination in one second is over a threshold, the destination is experiencing flooding. |
| Scan | If the number of sessions from a single source in one second is over a threshold, the source is scanning. |
| Source session limit | If the number of concurrent sessions from a single source is over a threshold, the source session limit is reached. |
| Destination session limit | If the number of concurrent sessions to a single destination is over a threshold, the destination session limit is reached. |

Enable or disable logging for each anomaly, and select the action taken in response to detecting an anomaly. Configure the anomaly thresholds to detect traffic patterns that could represent an attack.



It is important to estimate the normal and expected traffic on the network before changing the default anomaly thresholds. Setting the thresholds too low could cause false positives, and setting the thresholds too high could allow some attacks.

The list of anomalies can be updated only when the FortiGate firmware image is upgraded.

Syntax

```
config firewall DoS-policy
  edit <dospolicy_id_int>
    set client-reputation {enable | disable}
    set dstaddr <name_str>
    set interface <name_str>
    set service <name_str>
    set srcaddr <name_str>
    set status {enable | disable}
    config anomaly
      edit <anomaly_str>
        set action {block | pass}
        set log {enable | disable}
        set quarantine {attacker | both | interface | none}
        set status {enable | disable}
        set threshold <threshold_int>
      end
    end
  end
```

| Variable | Description | Default |
|---|---|-------------------|
| client-reputation {enable disable} | Enable or disable the client reputation feature in this policy. | disable |
| dstaddr <name_str> | Enter one or more destination firewall addresses. | No default. |
| interface <name_str> | Set the interface. | No default. |
| service <name_str> | Enter one or more services to which the policy applies. | No default. |
| srcaddr <name_str> | Enter one or more source firewall addresses. | No default. |
| status {enable disable} | Enable or disable the specified anomaly in the current DoS sensor. | disable |
| config anomaly fields | | |
| <anomaly_str> | Enter the name of the anomaly you want to configure. Display a list of the available anomaly types by entering '?'. | No default. |
| action {block pass} | Pass or block traffic in which the specified anomaly is detected. | pass |
| log {enable disable} | Enable or disable logging of the specified anomaly in the current DoS sensor. | disable |
| quarantine {attacker both interface none} | <p>To prevent the attacker from continuing to attack the FortiGate unit, you can quarantine the attacker to the banned user list in one of three ways.</p> <ul style="list-style-type: none"> Enter <code>attacker</code> to block all traffic sent from the attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected. Enter <code>both</code> to block all traffic sent from the attacker's IP address to the target (victim's) IP address. Traffic from the attacker's IP address to addresses other than the victim's IP address is allowed. The attacker's and target's IP addresses are added to the banned user list as one entry. Enter <code>interface</code> to block all traffic from connecting to the FortiGate unit interface that received the attack. The interface is added to the banned user list. Enter <code>none</code> to disable the adding of addresses to the quarantine but the current DoS sensor. | none |
| status {enable disable} | Enable or disable the specified anomaly in the current DoS sensor. | disable |
| threshold <threshold_int> | <p>Enter the number of times the specified anomaly must be detected in network traffic before the action is triggered.</p> <p>Range 1 to 2 147 483 647.</p> | varies by anomaly |

gtp

Use this command to configure GTP profiles. This command is FortiOS Carrier only.

Syntax

```
config firewall gtp
  edit <name_str>
    config apn
      edit index_int
        set action {allow | deny}
        set selection-mode {ms net vrf}
        set value <networkid_str>
      end
    config ie-remove-policy
      edit <index_int>
        set remove-ies {apn-restriction rat-type rai uli imei}
        set sgsn-addr <addr/group_str>
      end
    config ie-validation
      set apn-restriction {disable | enable}
      set charging-ID {disable | enable}
      set charging-gateway-addr {disable | enable}
      set end-user-addr {disable | enable}
      set gsn-addr {disable | enable}
      set imei {disable | enable}
      set imsi {disable | enable}
      set mm-context {disable | enable}
      set ms-tzone {disable | enable}
      set ms-validated {disable | enable}
      set msisdn {disable | enable}
      set nsapi {disable | enable}
      set pdp-context {disable | enable}
      set qos-profile {disable | enable}
      set rai {disable | enable}
      set rat-type {disable | enable}
      set reordering-required {disable | enable}
      set selection-mode {disable | enable}
      set uli {disable | enable}
    end
  config imsi
    edit <index_int>
      set action {allow | deny}
      set apn <networkid_str>
      set mcc-mnc <mccmnc_str>
      set selection-mode {ms net vrf}
    end
```

```
config ip-policy
  edit <index_int>
    set action {allow | deny}
    set dstaddr <address_str>
    set srcaddr <address_str>
  end
config message-filter
  edit <index_int>
    set create-aa-pdp {allow | deny}
    set create-mbms {allow | deny}
    set create-pdp {allow | deny}
    set data-record {allow | deny}
    set delete-aa-pdp {allow | deny}
    set delete-mbms {allow | deny}
    set delete-pdp {allow | deny}
    set echo {allow | deny}
    set error-indication {allow | deny}
    set failure-report {allow | deny}
    set fwd-relocation {allow | deny}
    set fwd-srns-context {allow | deny}
    set gtp-pdu {allow | deny}
    set identification {allow | deny}
    set mbms-notification {allow | deny}
    set node-alive {allow | deny}
    set note-ms-present {allow | deny}
    set pdu-notification {allow | deny}
    set ran-info {allow | deny}
    set redirection {allow | deny}
    set relocation-cancel {allow | deny}
    set send-route {allow | deny}
    set sgsn-context {allow | deny}
    set support-extension {allow | deny}
    set unknown-message-action {allow | deny}
    set update-mbms {allow | deny}
    set update-pdp {allow | deny}
    set version-not-support {allow | deny}
  end
config message-rate-limit
  edit <index_int>
    set
    set
    set
  end
config noip-policy
  edit <index_int>
    set action {allow | deny}
    set start <protocol_int>
    set end <protocol_int>
    set type {etsi | ietf}
```

```
end
config policy
edit <index_int>
    set action {allow | deny}
    set apn <apn_str>
    set imei <imei_str>
    set imsi <imsi_str>
    set max-apn-restriction {all | private-1 | private-2 |
        public-1 | public-2}
    set messages {create-req create-res update-req update-res}
    set rai <rai_str>
    set rat-type {any geran utran wlan}
    set uli <uli_str>
end
set addr-notify <Gi_ipv4>
set apn-filter {enable | disable}
set authorized-sgsns <addr/grp_str>
set context-id <id_int>
set control-plane-message-rate-limit <limit_int>
set create-aa-pdp {allow | deny}
set create-pdp {allow | deny}
set data-record {allow | deny}
set default-apn-action {allow | deny}
set default-imsi-action {allow | deny}
set default-ip-action {allow | deny}
set default-noip-action {allow | deny}
set default-policy-action {allow | deny}
set delete-aa-pdp {allow | deny}
set delete-pdp {allow | deny}
set denied-log {enable | disable}
set echo {allow | deny}
set error-indication {allow | deny}
set extension-log {enable | disable}
set failure-report {allow | deny}
set forwarded-log {enable | disable}
set fwd-relocation {allow | deny}
set fwd-srns-context {allow | deny}
set gtp-in-gtp {allow | deny}
set gtp-pdu {allow | deny}
set handover-group <group_name>
set identification {allow | deny}
set ie-remover {enable | disable}
set imsi-filter {enable | disable}
set interface-notify <interface_str>
set invalid-reserved-field {allow | deny}
set ip-filter {enable | disable}
set log-freq <drop_int>
set max-message-length <bytes_int>
set min-message-length <bytes_int>
```



```

set miss-must-ie {allow | deny}
set node-alive {allow | deny}
set noip-filter {enable | disable}
set note-ms-present {allow | deny}
set out-of-state-ie {allow | deny}
set out-of-state-message {allow | deny}
set pdu-notification {allow | deny}
set policy-filter {enable | disable}
set port-notify <port_int>
set ran-info {allow | deny}
set rate-limited-log {enable | disable}
set redirection {allow | deny}
set relocation-cancel {allow | deny}
set reserved-ie {allow | deny}
set send-route {allow | deny}
set seq-number-validate {enable | disable}
set sgsn-context {allow | deny}
set spoof-src-addr {allow | deny}
set state-invalid-log {enable | disable}
set support-extension {allow | deny}
set traffic-count-log {enable | disable}
set tunnel-limit <limit_int>
set tunnel-limit-log {enable | disable}
set tunnel-timeout <time_int>
set unknown-message-action {allow | deny}
set unknown-version-action {allow | deny}
set update-pdp {allow | deny}
set version-not-support {allow | deny}
end

```

| Variable | Description | Default |
|---|---|-------------|
| <name_str> | Enter the name of this GTP profile. | No default. |
| apn The following commands are the options for <code>config apn</code> . | | |
| index_int | Enter the unique ID number of the APN filter profile. | No default. |
| action {allow deny} | Select to allow or deny traffic matching both the APN and Selection Mode specified for this APN filter profile. | allow |

| Variable | Description | Default |
|---|---|---|
| selection-mode {ms net vrf} | <p>Select the selection mode or modes required for the APN. The selection mode indicates where the APN originated and whether the Home Location Register (HLR) has verified the user subscription.</p> <ul style="list-style-type: none"> Enter <code>ms</code> to specify a mobile station provided APN, subscription not verified. This Selection Mode indicates that the mobile station (MS) provided the APN and that the HLR did not verify the user's subscription to the network. Enter <code>net</code> to specify a network-provided APN, subscription not verified. This Selection Mode indicates that the network provided a default APN because the MS did not specify one, and that the HLR did not verify the user's subscription to the network. Enter <code>vrf</code> to specify a mobile station or network-provided APN, subscription verified. This Selection Mode indicates that the MS or the network provided the APN and that the HLR verified the user's subscription to the network. | ms net vrf |
| value <networkid_str> | Enter the network ID and operator ID of the APN. | No default. |
| ie-remove-policy The following commands are the <code>set</code> options for <code>config ie-remove-policy</code> . | | |
| <index_int> | Enter the unique ID number of the IE removal policy. | No default. |
| remove-ies {apn-restriction rat-type rai uli imei} | Select the information elements to be removed from messages prior to being forwarding to the HGGSN. Any combination of R6 information elements (RAT, RAI, ULI, IMEI-SV and APN restrictions) may be specified. | apn- restriction rat-type rai uli imei |
| sgsn-addr <addr/group_str> | Enter an SGSN address or group the IE removal policy will be applied to. | all |
| ie-validation The following commands allow validating specific parts of the IE | | |
| apn-restriction {disable enable} | <p>Enable to restrict the Access Point Number (APN).</p> <p>Restricting the APN limits the IP packet data networks that can be associated with the GTP tunnel.</p> | disable |
| charging-ID {disable enable} | Enable to validate the charging ID in the IE. | disable |
| charging-gateway-addr {disable enable} | Enable to validate the charging gateway address. | disable |
| end-user-addr {disable enable} | Enable to validate the end user address. | disable |
| gsn-addr {disable enable} | Enable to validate the GSN address. | disable |
| imei {disable enable} | Enable to validate the IMEI (SV). | disable |
| imsi {disable enable} | Enable to validate the IMSI. | disable |
| mm-context {disable enable} | Enable to validate the MM context. | disable |

| Variable | Description | Default |
|---|--|-------------|
| ms-tzone {disable enable} | Enable to validate the mobile station (MS) timezone. | disable |
| ms-validated {disable enable} | Enable to validate the MS. | disable |
| msisdn {disable enable} | Enable to validate the MSISDN. | disable |
| nsapi {disable enable} | Enable to validate the NSAPI. | disable |
| pdp-context {disable enable} | Enable to validate the PDP context. | disable |
| qos-profile {disable enable} | Enable to validate the Quality of Service (QoS). | disable |
| rai {disable enable} | Enable to validate the RAI. | disable |
| rat-type {disable enable} | Enable to validate the RAT type. | disable |
| reordering-required {disable enable} | Enable to validate the required reordering. | disable |
| selection-mode {disable enable} | Enable to validate the selection mode. | disable |
| uli {disable enable} | Enable to validate the User Location Information (ULI). | disable |
| imsi | | |
| The following commands are the options for <code>config imsi</code> . | | |
| <index_int> | Enter the unique ID number of the IMSI filtering policy. | disable |
| action {allow deny} | Select to allow or deny traffic matching both the APN and Selection Mode specified for this APN filter profile | allow |
| apn <networkid_str> | Enter the network ID and operator ID of the APN. | No default. |
| mcc-mnc <mccmnc_str> | Enter the MCC and MNC. | No default. |
| selection-mode {ms net vrf} | <p>Select the selection mode or modes. The selection mode indicates where the APN originated and whether the Home Location Register (HLR) has verified the user subscription.</p> <ul style="list-style-type: none"> Enter <code>ms</code> to specify a mobile station provided APN, subscription not verified. This Selection Mode indicates that the mobile station (MS) provided the APN and that the HLR did not verify the user's subscription to the network. Enter <code>net</code> to specify a network-provided APN, subscription not verified. This Selection Mode indicates that the network provided a default APN because the MS did not specify one, and that the HLR did not verify the user's subscription to the network. Enter <code>vrf</code> to specify a mobile station or network-provided APN, subscription verified. This Selection Mode indicates that the MS or the network provided the APN and that the HLR verified the user's subscription to the network. | ms net vrf |

| Variable | Description | Default |
|---|--|-------------|
| ip-policy The following commands are the options for <code>config ip-policy</code> . | | |
| <index_int> | Enter the unique ID number of the encapsulated IP traffic filtering policy. | No default. |
| action {allow deny} | Select to allow or deny traffic matching both the source and destination addresses specified for this APN filter profile | allow |
| dstaddr <address_str> | Enter the name of a destination address or address group. | No default. |
| srcaddr <address_str> | Enter the name of a source address or address group. | No default. |
| message-filter The following tunnel management messages are used to create, update and delete tunnels used to route tunneled PDUs between a MS and a PDN via SGSN and GGSN. | | |
| create-aa-pdp {allow deny} | Allow Anonymous Access Packet Data Protocol (AA PDP) tunnel management messages. These messages are used to create a tunnel between a context in the SGSN and context GGSN. | allow |
| create-mbms {allow deny} | Allow Multimedia Broadcast Multicast Service (MBMS) create messages. These messages occur when a GTP-U tunnel is setup for a multicast flow. | allow |
| create-pdp {allow deny} | Allow create PDP context tunnel management messages. Sent from a SGSN to a GGSN node as part of the GPRS PDP Context Activation procedure | allow |
| data-record {allow deny} | Allow data record messages. Data record messages are used to reliably transport CDRs from the point of generation (SGSN/GGSN) to non-volatile storage in the CGF | allow |
| delete-aa-pdp {allow deny} | Allow Anonymous Access (AA) PDP context tunnel management messages. These messages are sent between the SGSN and GGSN as part of the AA PDP context deactivation procedure. | allow |
| delete-mbms {allow deny} | Allow delete MBMS messages. These messages are part of the request to deactivate the MBMS context. When the response is received, the MBMS context will be inactive. | allow |
| delete-pdp {allow deny} | Allow delete PDP context tunnel management message. Messages are sent as part of the GPRS Detach Procedure to deactivate an activated PDP Context. | allow |
| echo {allow deny} | Allow Echo path management messages. These messages are sent to a GSN peer to see if it is alive. | allow |

| Variable | Description | Default |
|-----------------------------------|--|---------|
| error-indication { allow deny } | <p>Allow error indication message.</p> <p>These messages are sent to the GGSN when a tunnel PDU is received when</p> <ul style="list-style-type: none"> no PDP context exists PDP context is inactive no MM context exists GGSN deletes its PDP context when the message is received | allow |
| failure-report { allow deny } | <p>Allow failure report messages.</p> <p>The GGSN sends the failure report request, and the GSN sends the response. Causes for the failure can include:</p> <ul style="list-style-type: none"> request accepted no resources available service not supported system failure mandatory IE incorrect mandatory IE missing optional IE incorrect invalid message format version not supported | allow |
| fwd-relocation { allow deny } | <p>Allow forward relocation mobility management messages.</p> <p>These messages indicate mobile activation/deactivation within a Routing Area. This prevents paging of a mobile device that is not active (visited VLR rejects calls from the HLR or applies Call Forwarding). Note that the mobile station does not maintain an attach/detach state.</p> <p>SRNS contexts contain for each concerned RAB the sequence numbers of the GTP-PDUs next to be transmitted in uplink and downlink directions.</p> | allow |
| fwd-srns-context { allow deny } | <p>Allow forward SRNS context mobility management messages.</p> <p>This procedure may be used to trigger the transfer of SRNS contexts from RNC to CN (PS domain) in case of inter system forward handover.</p> | allow |
| gtp-pdu { allow deny } | Allow GPRS Packet data unit delivery management messages. | allow |
| identification { allow deny } | <p>Allow identification mobility management messages.</p> <p>If the mobile station (MS) identifies itself at GPRS attach, and the SGSN has changed since the detach, the new SGSN will send an identification message to the old SGSN to get the IMSI.</p> | allow |

| Variable | Description | Default |
|---|---|---------|
| mbms-notification { allow deny } | Allow MBMS notification MBMS messages. These are used for the notification of the radio access devices. | allow |
| node-alive { allow deny } | Allow node alive GTP-U messages. This message is used to inform the rest of the network when a node starts service. | allow |
| note-ms-present { allow deny } | Allow Note MS messages. This message is sent when an MS should be reachable for GPRS. | allow |
| pdu-notification { allow deny } | Allow PDU notification messages including response, request, and reject response. These messages are sent between the GGSN and SGSN as part of the new PDP context initiation procedure. | allow |
| ran-info { allow deny } | Allow Radio Access Network (RAN) information messages. | allow |
| redirection { allow deny } | Allow redirection GTP-U messages. Used to divert the flow of CDRs from the CDFs to another CGF when the sender is being removed, or they are used when the CGF has lost its connection to a downstream system. | allow |
| relocation-cancel { allow deny } | Allow relocation cancel mobility messages. Send to cancel the relocation of a connection. | allow |
| send-route { allow deny } | Allow Send Routing information for GPRS messages. This message is sent to get the IP address of the SGSN where the MS is located when there is no PDP context. | allow |
| sgsn-context { allow deny } | Allow Serving GPRS Support Node (SGSN) context request, response, and acknowledge messages. The new SGSN will send this message to the old SGSN to get the Mobility Management (MM) and PDP contexts for the MS. | allow |
| support-extension { allow deny } | Allow messages about support various header extensions. | allow |
| unknown-message-action { allow deny } | Allow unknown message action messages. This message type needs to be set to deny as that will prevent malformed messages which may be attempts to hack into the network. | allow |
| update-mbms { allow deny } | Allow MBMS update messages. | allow |
| update-pdp { allow deny } | Allow Update PDP context tunnel management messages. Messages sent as part of the GPRS Inter-SGSN Routing Update procedure, and is used to change the QoS and the path. | allow |

| Variable | Description | Default |
|---|---|---------|
| version-not-support {allow deny} | Allow version not supported path management messages. This message indicates the more recent version of GTP that is supported. | allow |
| message-rate-limit The following commands are rate limits in packets per second for various message context requests and responses. A rate of zero indicates there is no rate limiting in place. | | |
| create-aa-pdp-request | | 0 |
| create-aa-pdp-response | | 0 |
| create-mbms-request | | 0 |
| create-mbms-response | | 0 |
| create-pdp-request | | 0 |
| create-pdp-response | | 0 |
| delete-aa-pdp-request | | 0 |
| delete-aa-pdp-response | | 0 |
| delete-mbms-request | | 0 |
| delete-mbms-response | | 0 |
| delete-pdp-request | | 0 |
| delete-pdp-response | | 0 |
| echo-reponse | | 0 |
| echo-request | | 0 |
| error-indication | | 0 |
| failure-report-request | | 0 |
| failure-report-response | | 0 |
| fwd-reloc-complete-ack | | 0 |
| fwd-relocation-complete | | 0 |
| fwd-relocation-request | | 0 |
| fwd-relocation-response | | 0 |
| fwd-srns-context | | 0 |
| fwd-srns-context-ack | | 0 |
| g-pdu | | 0 |
| identification-request | | 0 |
| identification-response | | 0 |
| mbms-de-reg-request | | 0 |
| mbms-de-reg-response | | 0 |
| mbms-notify-rej-request | | 0 |
| mbms-notify-rej-response | | 0 |
| mbms-notify-request | | 0 |
| mbms-notify-response | | 0 |
| mbms-reg-request | | 0 |
| mbms-reg-response | | 0 |
| mbms-ses-start-request | | 0 |

| Variable | Description | Default |
|--|--|-------------|
| mbms-ses-start-response | | 0 |
| mbms-ses-stop-request | | 0 |
| mbms-ses-stop-response | | 0 |
| note-ms-request | note ms GPRS present request | 0 |
| note-ms-response | note ms GPRS present response | 0 |
| pdu-notify-rej-request | | 0 |
| pdu-notify-rej-response | rate limit (packs/s) for pdu notification reject response | 0 |
| pdu-notify-request | | 0 |
| pdu-notify-response | | 0 |
| ran-info | RAN information relay | 0 |
| relocation-cancel-request | | 0 |
| relocation-cancel-response | | 0 |
| send-route-request | | 0 |
| send-route-response | | 0 |
| sgsn-context-ack | | 0 |
| sgsn-context-request | | 0 |
| sgsn-context-response | | 0 |
| support-ext-hdr-notify | | 0 |
| update-mbms-request | | 0 |
| update-mbms-response | | 0 |
| update-pdp-request | | 0 |
| update-pdp-response | | 0 |
| version-not-support | | 0 |
| noip-policy | | |
| The following commands are the options for <code>config noip-policy</code> . | | |
| <index_int> | Enter the unique ID number of the encapsulated non-IP traffic filtering policy. | No default. |
| action { allow deny } | Select to allow or deny traffic matching the message protocol specified for this APN filter profile | allow |
| start <protocol_int> | Enter the number of the start protocol. Acceptable rate values range from 0 to 255. | 0 |
| end <protocol_int> | Enter the number of the end protocol. Acceptable rate values range from 0 to 255. | 0 |
| type { etsi ietf } | Select an ETSI or IETF protocol type. | etsi |
| policy | | |
| The following commands are the options for <code>config policy</code> . | | |
| <index_int> | Enter the unique ID number of the advanced filtering policy. | No default. |
| action { allow deny } | Select to allow or deny traffic matching the message attributes specified for this advanced filtering policy | allow |
| apn <apn_str> | Enter the APN suffix, if required. | No default. |
| imei <imei_str> | Enter the IMEI (SV) pattern, if required. | No default. |

| Variable | Description | Default |
|---|---|-------------|
| imsi <imsi_str> | Enter the IMSI prefix, if required. | No default. |
| max-apn-restriction { all private-1 private-2 public-1 public-2 } | Select the maximum APN restriction. | all |
| messages { create-req create-res update-req update-res } | Enter the type or types of GTP messages. | create-req |
| rai <rai_str> | Enter the Routing Area Identifier (RAI) pattern. The RAI and ULI are commonly used to determine a mobile user's location. | No default. |
| rat-type { any geran utran wlan } | Enter one or more Radio Access Technology (RAT) types. <ul style="list-style-type: none"> any - accept any RAT type geran - GSM EDGE Radio Access Network utran - UMTS Terrestrial Radio Access Network wlan - Wireless LAN | any |
| uli <uli_str> | Enter the ULI pattern. | No default. |
| The following commands are the options for edit <profile_str>. | | |
| addr-notify <Gi_ipv4> | Enter the IP address of the Gi firewall. | 0.0.0.0 |
| apn-filter { enable disable } | Select to apply APN filter policies. | disable |
| authorized-sgsns <addr/grp_str> | Enter authorized SSGN addresses or groups. Any SSGN groups not specified will not be able to send packets to the GGSN. All firewall addresses and groups defined on the FortiGate unit are available for use with this command. | all |
| context-id <id_int> | Enter the security context ID. This ID must match the ID entered on the server Gi firewall. | 696 |
| control-plane-message-rate-limit <limit_int> | Enter the control plane message rate limit. Acceptable rate values range from 0 (no limiting) to 2147483674 packets per second. FortiGate units can limit the packet rate to protect the GSNs from possible Denial of Service (DoS) attacks, such as Border gateway bandwidth saturation or a GTP flood. | 0 |
| create-aa-pdp { allow deny } | Select to allow or deny all create AA pdp messages. | allow |
| create-pdp { allow deny } | Select to allow or deny all create pdp messages. | allow |
| data-record { allow deny } | Select to allow or deny all data record messages. | allow |
| default-apn-action { allow deny } | Select to allow or deny any APN that is not explicitly defined with in an APN policy. | allow |
| default-imsi-action { allow deny } | Select to allow or deny any IMSI that is not explicitly defined in an IMSI policy. | allow |
| default-ip-action { allow deny } | Select to allow or deny any encapsulated IP address traffic that is not explicitly defined in an IP policy. | allow |

| Variable | Description | Default |
|---|--|-------------|
| default-noip-action { allow deny } | Select to allow or deny any encapsulated non-IP protocol that is not explicitly defined in a non-IP policy. | allow |
| default-policy-action { allow deny } | Select to allow or deny any traffic that is not explicitly defined in an advanced filtering policy. | allow |
| delete-aa-pdp { allow deny } | Select to allow or deny all delete AA pdp messages. | allow |
| delete-pdp { allow deny } | Select to allow or deny all delete pdp messages. | allow |
| denied-log { enable disable } | Select to log denied GTP packets. | disable |
| echo { allow deny } | Select to allow or deny all echo messages. | allow |
| error-indication { allow deny } | Select to allow or deny all error indication messages. | allow |
| extension-log { enable disable } | Select to log extended information about GTP packets. When enabled, this additional information will be included in log entries: <ul style="list-style-type: none"> • IMSI • MSISDN • APN • Selection Mode • SGSN address for signaling • SGSN address for user data • GGSN address for signaling • GGSN address for user data | disable |
| failure-report { allow deny } | Select to allow or deny all failure report messages. | allow |
| forwarded-log { enable disable } | Select to log forwarded GTP packets. | disable |
| fwd-relocation { allow deny } | Select to allow or deny all forward relocation messages. | allow |
| fwd-srns-context { allow deny } | Select to allow or deny all forward SRNS messages. | allow |
| gtp-in-gtp { allow deny } | Select to allow or deny GTP packets that contains another GTP packet in its message body. | allow |
| gtp-pdu { allow deny } | Select to allow or deny all G-PDU messages. | allow |
| handover-group <group_name> | Handover requests will be honored only from the addresses listed in the specified address group. This way, an untrusted GSN cannot highjack a GTP tunnel with a handover request. | No default. |
| identification { allow deny } | Select to allow or deny all identification messages. | allow |
| ie-remover { enable disable } | Select whether to use information element removal policies. | disable |
| imsi-filter { enable disable } | Select whether to use IMSI filter policies. | disable |

| Variable | Description | Default |
|--|--|---------|
| interface-notify <interface_str> | Enter any local interface of the FortiGate unit. The interface IP address will be used to send the “clear session” message. | |
| invalid-reserved-field {allow deny} | Select to allow or deny GTP packets with invalid reserved fields. Depending on the GTP version, a varying number of header fields are reserved and should contain specific values. If the reserved fields contain incorrect values, the packet will be blocked if this field is set to <code>deny</code> . | deny |
| ip-filter {enable disable} | Select whether to use encapsulated IP traffic filtering policies. | disable |
| log-freq <drop_int> | Enter the number of messages to drop between logged messages. An overflow of log messages can sometimes occur when logging rate-limited GTP packets exceed their defined threshold. To conserve resources on the syslog server and the FortiGate unit, you can specify that some log messages are dropped. For example, if you want only every twentieth message to be logged, set a logging frequency of 19. This way, 19 messages are skipped and the next logged. Acceptable frequency values range from 0 to 2147483674. When set to ‘0’, no messages are skipped. | 0 |
| max-message-length <bytes_int> | Enter the maximum GTP message size, in bytes, that the FortiGate unit will allow to pass. Acceptable values range from 0 to 2147483674 bytes. When set to ‘0’, the maximum size restriction is disabled. | 1452 |
| min-message-length <bytes_int> | Enter the minimum GTP message size, in bytes, that the FortiGate unit will allow to pass. Acceptable values range from 0 to 2147483674 bytes. When set to ‘0’, the minimum size restriction is disabled. | 0 |
| miss-must-ie {allow deny} | Select to allow or deny passage of GTP packets with missing mandatory information elements to the GGSN. | deny |
| node-alive {allow deny} | Select to allow or deny all node alive messages. | allow |
| noip-filter {enable disable} | Enable or disable the configured encapsulated non-IP traffic filtering policies. | disable |
| note-ms-present {allow deny} | Select to allow or deny all note MS GPRS present messages. | allow |
| out-of-state-ie {allow deny} | Select to allow or deny passage of GTP Packets with out of sequence information elements. | deny |
| out-of-state-message {allow deny} | Select to allow or deny out of state messages. The GTP protocol requires a certain state to be kept by both the GGSN and SGSN. Since the GTP has a state, some message types can only be sent when in specific states. Packets that do not make sense in the current state should be filtered or rejected | deny |

| Variable | Description | Default |
|---|---|---------|
| pdu-notification { allow deny } | Select to allow or deny all pdu notification messages. | allow |
| policy-filter { enable disable } | Enable or disable the configured advanced filtering policies. | disable |
| port-notify <port_int> | Enter the server firewall's listening port number. | 21123 |
| ran-info { allow deny } | Select to allow or deny all RAN info relay messages. | allow |
| rate-limited-log { enable disable } | Select to log rate-limited GTP packets. | disable |
| redirection { allow deny } | Select to allow or deny all redirection messages. | allow |
| relocation-cancel { allow deny } | Select to allow or deny all relocation cancel messages. | allow |
| reserved-ie { allow deny } | Select to allow or deny GTP messages with reserved or undefined information elements. | deny |
| send-route { allow deny } | Select to allow or deny all send route messages. | allow |
| seq-number-validate { enable disable } | Enable or disable sequence number validation The GTP packet header contains a sequence number. The receiving GGSN and the sending GGSN use this number to ensure the packets are in sequence. The FortiGate unit can assume this task and save GGSN resources. | disable |
| sgsn-context { allow deny } | Select to allow or deny all SGSN context messages. | allow |
| spoof-src-addr { allow deny } | Select to allow or deny packets containing spoofed MS addresses. As the MS address is negotiated within the PDP Context creation handshake, any packets originating from the MS that contain a different source address will be detected and dropped if this field is set to deny. | deny |
| state-invalid-log { enable disable } | Select to log GTP packets that have failed stateful inspection. | disable |
| support-extension { allow deny } | Select to allow or deny all support extension messages. | allow |
| traffic-count-log { enable disable } | Enable or disable logging the total number of control and user data messages received from and forwarded to the GGSNs and SGSNs the FortiGate unit protects. | disable |
| tunnel-limit <limit_int> | Enter the maximum number of GTP tunnels according to the GSN capacity. | 0 |
| tunnel-limit-log { enable disable } | Select to log packets dropped because the maximum limit of GTP tunnels for the destination GSN is reached. | disable |
| tunnel-timeout <time_int> | Enter a tunnel timeout value, in seconds. By setting a timeout value, you can configure the FortiGate unit to remove hanging tunnels. Acceptable values range from 0 to 2147483674 seconds. When set to '0', the timeout is disabled. | 86400 |
| unknown-message-action { allow deny } | Select to allow or deny all unknown message types. | allow |
| unknown-version-action { allow deny } | Select to allow or deny traffic with GTP version higher than 1. | allow |

| Variable | Description | Default |
|---------------------------------------|---|---------|
| update-pdp {allow deny} | Select to allow or deny all update pdp messages. | allow |
| version-not-support {allow deny} | Select to allow or deny all version not supported messages. | allow |

identity-based-route

Use this command to define identity-based routes.

Syntax

```
config firewall identity-based-route
edit <route_name_str>
set comments <comment_str>
config rule
edit <id_int>
set device <interface>
set gateway <ip4_addr>
set groups <group_list>
end
end
```

| Variable | Description | Default |
|---------------------------|--|-------------|
| <route_name_str> | | No default. |
| comments <comment_str> | | No default. |
| device <interface> | Enter the output interface for this route. | No default. |
| gateway <ip4_addr> | Enter the gateway IP address. | 0.0.0.0 |
| groups <group_list> | Enter the groups who are allowed to use this route. Separate group names with spaces. | No default. |

interface-policy

DoS policies, called interface policies in the CLI, are primarily used to apply DoS sensors to network traffic based on the FortiGate interface it is leaving or entering as well as the source and destination addresses. DoS sensors are a traffic anomaly detection feature to identify network traffic that does not fit known or common traffic patterns and behavior. A common example of anomalous traffic is the denial of service attack. A denial of service occurs when an attacking system starts an abnormally large number of sessions with a target system. The large number of sessions slows down or disables the target system so legitimate users can no longer use it. You can also use the `Interface-policy` command to invoke an IPS sensor as part of a DoS policy.

The `interface-policy` command is used for DoS policies applied to IPv4 addresses. For IPv6 addresses, use `interface-policy6` instead.

Syntax

```
config firewall interface-policy
  edit <policy_id>
    set application-list-status {enable | disable}
    set application_list <app_list_str>
    set av-profile-status {enable | disable}
    set av-profile <avprofile_name>
    set dlp-profile-status {enable | disable}
    set dlp-profile <avprofile_name>
    set dstaddr <dstaddr_ipv4>
    set interface <int_str>
    set ips-sensor-status {enable | disable}
    set ips-sensor <sensor_str>
    set service <service_str>
    set spamfilter-profile <spfilter_profile_name>
    set spamfilter-profile-status {enable | disable}
    set srcaddr <srcaddr_ipv4>
    set status {enable | disable}
    set webfilter-profile-status {enable | disable}
    set webfilter-profile <webfilter_profile_name>
  end
```

| Variable | Description | Default |
|---|---|-------------|
| application-list-status {enable disable} | Enable to have the FortiGate unit apply an application black/white list to matching network traffic. | disable |
| application_list <app_list_str> | Enter the name of the application black/white list the FortiGate unit uses when examining network traffic. This option is available only when <code>application-list-status</code> is set to <code>enable</code> . | No default. |
| av-profile-status {enable disable} | Enable to apply an antivirus profile to traffic on this interface. | disable |
| av-profile <avprofile_name> | Enter the antivirus profile to apply. This is available when <code>av-profile-status</code> is enabled. | No default. |
| dlp-profile-status {enable disable} | Enable to apply a Data Leak Prevention (DLP) profile to traffic on this interface. | disable |

| Variable | Description | Default |
|---|--|-------------|
| dlp-profile <avprofile_name> | Enter the Data Leak Prevention (DLP) profile to apply. This is available when dlp-profile-status is enabled. | No default. |
| dstaddr <dstaddr_ipv4> | Enter an address or address range to limit traffic monitoring to network traffic sent to the specified address or range. | |
| interface <int_str> | The interface or zone to be monitored. | |
| ips-sensor-status { enable disable } | Enable to have the FortiGate unit examine network traffic for attacks and vulnerabilities. | disable |
| ips-sensor <sensor_str> | Enter the name of the IPS sensor the FortiGate unit will use when examining network traffic. This option is available only when ips-sensor-status is set to enable. | No default. |
| service <service_str> | Enter a service to limit traffic monitoring to only the selected type. You may also specify a service group, or multiple services separated by spaces. | No default. |
| spamfilter-profile <spfilter_profile_name> | Enter the spamfilter profile to apply. This is available when spamfilter-profile-status is enabled. | No default. |
| spamfilter-profile-status { enable disable } | Enable to apply a spamfilter profile to traffic on this interface. | disable |
| srcaddr <srcaddr_ipv4> | Enter an address or address range to limit traffic monitoring to network traffic sent from the specified address or range. | No default. |
| status { enable disable } | Enable or disable the DoS policy. A disabled DoS policy has no effect on network traffic. | enable |
| webfilter-profile-status { enable disable } | Enable to apply a webfilter profile to traffic on this interface. | disable |
| webfilter-profile <webfilter_profile_name> | Enter the webfilter profile to apply. This is available when webfilter-profile-status is enabled. | No default. |

interface-policy6

DoS policies (called interface policies in the CLI) for IPv6 addresses, are used to apply IPS sensors to network traffic based on the FortiGate interface it is leaving or entering as well as the source and destination addresses.

The `interface-policy6` command is used for DoS policies applied to IPv6 addresses. For IPv4 addresses, use `interface-policy` instead.

Syntax

```
config firewall interface-policy6
  edit <policy_id>
    set application-list-status {enable | disable}
    set application_list <app_list_str>
    set av-profile-status {enable | disable}
    set av-profile <avprofile_name>
    set dlp-profile-status {enable | disable}
    set dlp-profile <avprofile_name>
    set dstaddr6 <dstaddr_ipv6>
    set interface
    set ips-sensor-status {enable | disable}
    set ips-sensor <sensor_str>
    set service6 <service_str>
    set spamfilter-profile <spfilter_profile_name>
    set spamfilter-profile-status {enable | disable}
    set srcaddr6 <srcaddr_ipv6>
    set status {enable | disable}
    set webfilter-profile-status {enable | disable}
    set webfilter-profile <webfilter_profile_name>
  end
```

| Variable | Description | Default |
|---|--|-------------|
| application-list-status {enable disable} | Enable to have the FortiGate unit apply an application black/white list to matching network traffic. | disable |
| application_list <app_list_str> | Enter the name of the application black/white list the FortiGate unit uses when examining network traffic. This option is available only when application-list-status is set to enable. | No default. |
| av-profile-status {enable disable} | Enable to apply an antivirus profile to traffic on this interface. | disable |
| av-profile <avprofile_name> | Enter the antivirus profile to apply. This is available when av-profile-status is enabled. | No default. |
| dlp-profile-status {enable disable} | Enable to apply a Data Leak Prevention (DLP) profile to traffic on this interface. | disable |
| dlp-profile <avprofile_name> | Enter the Data Leak Prevention (DLP) profile to apply. This is available when dlp-profile-status is enabled. | No default. |

| Variable | Description | Default |
|---|---|-------------|
| dstaddr6 <dstaddr_ipv6> | Enter an address or address range to limit traffic monitoring to network traffic sent to the specified address or range. | |
| interface | The interface or zone to be monitored. | No default. |
| ips-sensor-status { enable disable } | Enable to have the FortiGate unit examine network traffic for attacks and vulnerabilities. | disable |
| ips-sensor <sensor_str> | Enter the name of the IPS sensor the FortiGate unit will use when examining network traffic. This option is available only when <code>ips-sensor-status</code> is set to <code>enable</code> . | No default. |
| service6 <service_str> | Enter a service to limit traffic monitoring to only the selected type. You may also specify a service group, or multiple services separated by spaces. | |
| spamfilter-profile <spfilter_profile_name> | Enter the spamfilter profile to apply. This is available when <code>spamfilter-profile-status</code> is enabled. | No default. |
| spamfilter-profile-status { enable disable } | Enable to apply a spamfilter profile to traffic on this interface. | disable |
| srcaddr6 <srcaddr_ipv6> | Enter an address or address range to limit traffic monitoring to network traffic sent from the specified address or range. | |
| status { enable disable } | Enable or disable the DoS policy. A disabled DoS policy has no effect on network traffic. | enable |
| webfilter-profile-status { enable disable } | Enable to apply a webfilter profile to traffic on this interface. | disable |
| webfilter-profile <webfilter_profile_name> | Enter the webfilter profile to apply. This is available when <code>webfilter-profile-status</code> is enabled. | No default. |

ipmacbinding setting

Use this command to configure IP to MAC address binding settings.

IP/MAC binding protects the FortiGate unit and/or the network from IP address spoofing attacks. IP spoofing attacks attempt to use the IP address of a trusted computer to connect to, or through, the FortiGate unit from a different computer. It is simple to change a computer's IP address to mimic that of a trusted host, but MAC addresses are often added to Ethernet cards at the factory, and are more difficult to change. By requiring that traffic from trusted hosts reflect both the IP address and MAC address known for that host, fraudulent connections are more difficult to construct.

To configure the table of IP addresses and the MAC addresses bound to them, see [“ipmacbinding table” on page 140](#). To enable or disable IP/MAC binding for an individual FortiGate unit network interface, see `ipmac` in [“system interface” on page 555](#).



If IP/MAC binding is enabled, and the IP address of a host with an IP or MAC address in the IP/MAC table is changed, or a new computer is added to the network, update the IP/MAC table. If you do not update the IP/MAC binding list, the new or changed hosts will not have access to or through the FortiGate unit. For details on updating the IP/MAC binding table, see [“ipmacbinding table” on page 140](#).



If a client receives an IP address from the FortiGate unit's DHCP server, the client's MAC address is automatically registered in the IP/MAC binding table. This can simplify IP/MAC binding configuration, but can also neutralize protection offered by IP/MAC binding if untrusted hosts are allowed to access the DHCP server. Use caution when enabling and providing access to the DHCP server.

Syntax

```
config firewall ipmacbinding setting
    set bindthroughfw {enable | disable}
    set bindtofw {enable | disable}
    set undefinedhost {allow | block}
end
```

| Variable | Description | Default |
|-------------------------------------|---|---------|
| bindthroughfw {enable disable} | Select to use IP/MAC binding to filter packets that a firewall policy would normally allow through the FortiGate unit. | disable |
| bindtofw {enable disable} | Select to use IP/MAC binding to filter packets that would normally connect to the FortiGate unit. | disable |
| undefinedhost {allow block} | <p>Select how IP/MAC binding handles packets with IP and MAC addresses that are not defined in the IP/MAC list for traffic going through or to the FortiGate unit.</p> <ul style="list-style-type: none"> <code>allow</code>: Allow packets with IP and MAC address pairs that are not in the IP/MAC binding list. <code>block</code>: Block packets with IP and MAC address pairs that are not in the IP/MAC binding list. <p>This option is available only when either or both <code>bindthroughfw</code> and <code>bindtofw</code> are enable.</p> | block |

ipmacbinding table

Use this command to configure IP and MAC address pairs in the IP/MAC binding table. You can bind multiple IP addresses to the same MAC address, but you cannot bind multiple MAC addresses to the same IP address.

To configure the IP/MAC binding settings, see [“ipmacbinding setting” on page 139](#). To enable or disable IP/MAC binding for an individual FortiGate unit network interface, see `ipmac` in [“system interface” on page 555](#).



If IP/MAC binding is enabled, and the IP address of a host with an IP or MAC address in the IP/MAC table is changed, or a new computer is added to the network, update the IP/MAC table. If you do not update the IP/MAC binding list, the new or changed hosts will not have access to or through the FortiGate unit.



If a client receives an IP address from the FortiGate unit's DHCP server, the client's MAC address is automatically registered in the IP/MAC binding table. This can simplify IP/MAC binding configuration, but can also neutralize protection offered by IP/MAC binding if untrusted hosts are allowed to access the DHCP server. Use caution when enabling and providing access to the DHCP server.

Syntax

```
config firewall ipmacbinding table
  edit <index_int>
    set ip <address_ipv4>
    set mac <address_hex>
    set name <name_str>
    set status {enable | disable}
  end
```

| Variable | Description | Default |
|------------------------------|---|-------------------|
| <index_int> | Enter the unique ID number of this IP/MAC pair. | No default. |
| ip <address_ipv4> | Enter the IP address to bind to the MAC address. To allow all packets with the MAC address, regardless of the IP address, set the IP address to 0.0.0.0. | 0.0.0.0 |
| mac <address_hex> | Enter the MAC address. To allow all packets with the IP address, regardless of the MAC address, set the MAC address to 00:00:00:00:00:00. | 00:00:00:00:00:00 |
| name <name_str> | Enter a name for this entry on the IP/MAC address table. (Optional.) | noname |
| status {enable disable} | Select to enable this IP/MAC address pair. Packets not matching any IP/MAC binding will be dropped. Packets matching an IP/MAC binding will be matched against the firewall policy list. | disable |

ippool, ippool6

Use the `firewall ippool` command to configure IPv4 IP address pools.

Use the `firewall ippool6` command to configure IPv6 IP address pools.

Use IP pools to add NAT policies that translate source addresses to addresses randomly selected from the IP pool, rather than the IP address assigned to that FortiOS™ unit interface. In Transparent mode, IP pools are available only from the FortiGate CLI.

An IP pool defines a single IP address or a range of IP addresses. A single IP address in an IP pool becomes a range of one IP address. For example, if you enter an IP pool as 1.1.1.1 the IP pool is actually the address range 1.1.1.1 to 1.1.1.1.

If a FortiGate interface IP address overlaps with one or more IP pool address ranges, the interface responds to ARP requests for all of the IP addresses in the overlapping IP pools.

For example, consider a FortiGate unit with the following IP addresses for the port1 and port2 interfaces:

- port1 IP address: 1.1.1.1/255.255.255.0 (range is 1.1.1.0-1.1.1.255)
- port2 IP address: 2.2.2.2/255.255.255.0 (range is 2.2.2.0-2.2.2.255)

And the following IP pools:

- IP_pool_1: 1.1.1.10-1.1.1.20
- IP_pool_2: 2.2.2.10-2.2.2.20
- IP_pool_3: 2.2.2.30-2.2.2.40

The port1 interface overlap IP range with IP_pool_1 is:

- (1.1.1.0-1.1.1.255) and (1.1.1.10-1.1.1.20) = 1.1.1.10-1.1.1.20

The port2 interface overlap IP range with IP_pool_2 is:

- (2.2.2.0-2.2.2.255) & (2.2.2.10-2.2.2.20) = 2.2.2.10-2.2.2.20

The port2 interface overlap IP range with IP_pool_3 is:

- (2.2.2.0-2.2.2.255) & (2.2.2.30-2.2.2.40) = 2.2.2.30-2.2.2.40

And the result is:

- The port1 interface answers ARP requests for 1.1.1.10-1.1.1.20
- The port2 interface answers ARP requests for 2.2.2.10-2.2.2.20 and for 2.2.2.30-2.2.2.40

Select *NAT* in a firewall policy and then select *Dynamic IP Pool* and select an IP pool to translate the source address of packets leaving the FortiGate unit to an address randomly selected from the IP pool.

Syntax

```

config firewall ippool
  edit <ippool_name_str>
    set arp-intf <interface_name>
    set arp-reply {enable | disable}
    set block-size <size_int>
    set endip <address_ipv4>
    set num-blocks-per-user <int>
    set startip <address_ipv4>
    set source-endip <address_ipv4>
    set source-startip <address_ipv4>
    set type {one-to-one | overload | fixed-port-range
              | port-block-allocation}
  end

```

| Variable | Description | Default |
|--|---|-------------|
| <ippool_name_str> | Enter a name for this IP pool. | No default. |
| arp-intf <interface_name> | Send ARP replies only to the specified interface. Leave unset to send replies to all interfaces. arp-reply must be enabled. | Null |
| arp-reply {enable disable} | Enable or disable ARP replies. | enable |
| block-size <size_int> | Set the size of the port block. Available when type is port-block-allocation. Range 64 to 4096 | 128 |
| endip <address_ipv4> | The end IP of the address range. The end IP must be higher than the start IP. The end IP does not have to be on the same subnet as the IP address of the interface for which you are adding the IP pool. | 0.0.0.0 |
| num-blocks-per-user <int> | Set the number of ports per user when when type is port-block-allocation. Range: 1 to 128. | 8 |
| source-startip <address_ipv4> | Enter start IP for the range when type is fixed-port-range. | 0.0.0.0 |
| source-endip <address_ipv4> | Enter end IP for the range when type is fixed-port-range. | 0.0.0.0 |
| startip <address_ipv4> | The start IP of the address range. The start IP does not have to be on the same subnet as the IP address of the interface for which you are adding the IP pool. | 0.0.0.0 |
| type {one-to-one overload fixed-port-range port-block-allocation} | <p>Select the type of IP pool:</p> <p>one-to-one — one-to-one mapping</p> <p>overload — clients can share pool IP addresses</p> <p>fixed-port-range — fixed mapping of source-startip / source-endip range to startip / endip range.</p> <p>port-block-allocation — allocate a block of ports for IP pool users</p> | overload |

ip-translation

Use this command to configure IP address translation.

Syntax

```
config firewall ip-translation
edit <iptrans_id>
    set endip <ipv4_addr>
    set map-startip
    set startip <ipv4_addr>
end
```

| Variable | Description | Default |
|---------------------|---|-------------|
| <iptrans_id> | Enter an ID number for this IP address translation. | No default. |
| endip <ipv4_addr> | Enter the end of the IP address range to translate. | 0.0.0.0 |
| map-startip | Enter the beginning of the mapped address range. | 0.0.0.0 |
| startip <ipv4_addr> | Enter the beginning of the IP address range to translate. | 0.0.0.0 |

ipv6-eh-filter

Use this command to configure IPv6 routing header packet filtering.

Syntax

```
config firewall ipv6-eh-filter
  set hop-opt {enable | disable}
  set dest-opt {enable | disable}
  set hdopt-type <type_int_list>
  set routing {enable | disable}
  set routing-type <type_int_list>
  set fragment {enable | disable}
  set auth {enable | disable}
  set no-next {enable | disable}
end
```

| Variable | Description | Default |
|---------------------------------|--|---------|
| hop-opt {enable disable} | Enable to block packets with Hop-by-Hop Options header. | disable |
| dest-opt {enable disable} | Enable to block packets with Destination Options header. | disable |
| hdopt-type <type_int_list> | Enable to block specific Hop-by-Hop and/or Destination Option types. Types are integers, separate type values with spaces. | 0 |
| routing {enable disable} | Enable to block packets with Routing header. | enable |
| routing-type <type_int_list> | Enable to block specific Routing header types (maximum 7 types, each between 0 and 255). Types are integers, separate type values with spaces. | 0 |
| fragment {enable disable} | Enable to block packets with Fragment header. | disable |
| auth {enable disable} | Enable to block packets with Authentication header. | disable |
| no-next {enable disable} | Enable to block packets with No Next header. | disable |

ldb-monitor

Use this command to configure health check settings.

Health check settings can be used by load balancing VIPs to determine if a real server is currently responsive before forwarding traffic. One health check is sent per interval using the specified protocol, port and HTTP-GET, where applicable to the protocol. If the server does not respond during the timeout period, the health check fails and, if retries are configured, another health check is performed. If all health checks fail, the server is deemed unavailable, and another real server is selected to receive the traffic according to the selected load balancing algorithm.

Health check settings can be re-used by multiple real servers. For details on enabling health checking and using configured health check settings, see [“firewall vip” on page 222](#).

Syntax

```
config firewall ldb-monitor
edit <name_str>
    set http-get <httprequest_str>
    set http-match <contentmatch_str>
    set interval <seconds_int>
    set port <port_int>
    set retry <retries_int>
    set timeout <seconds_int>
    set type {http | ping | tcp}
end
```

| Variable | Description | Default |
|-------------------------------|--|-------------|
| <name_str> | Enter the name of the health check monitor. | No default. |
| http-get <httprequest_str> | <p>For HTTP health check monitors, add a URL that the FortiGate unit uses when sending a get request to check the health of a HTTP server. The URL should match an actual URL for the real HTTP servers. The URL is optional.</p> <p>The URL would not usually include an IP address or domain name. Instead it should start with a /and be followed by the address of an actual web page on the real server. For example, if the IP address of the real server is 10.10.10.1, the URL /test_page.htm causes the FortiGate unit to send an HTTP get request to http://10.10.10.1/test_page.htm.</p> <p>This option appears only if type is http.</p> | No default. |

| Variable | Description | Default |
|----------------------------------|--|-------------|
| http-match <contentmatch_str> | <p>For HTTP health check monitors, add a phrase that a real HTTP server should include in response to the get request sent by the FortiGate unit using the content of the http-get option. If the</p> <p>http-get URL returns a web page, the http-match option should exactly match some of the text on the web page. You can use the http-get and http-matched options to verify that an HTTP server is actually operating correctly by responding to get requests with expected web pages. http-match is only required if you add a http-get URL.</p> <p>For example, you can set http-match to "server test page" if the real HTTP server page defined by http-get contains the phrase server test page. When the FortiGate unit receives the web page in response to the URL get request, the system searches the content of the web page for the http-match phrase.</p> <p>This option appears only if type is http.</p> | No default. |
| interval <seconds_int> | Enter the interval time in seconds between health checks. | 10 |
| port <port_int> | <p>Enter the port number used to perform the health check. If you set the port to 0, the health check monitor uses the port defined in the real server. This way you can use a single health check monitor for different real servers.</p> <p>This option does not appear if type is ping.</p> | 0 |
| retry <retries_int> | Enter the number of times that the FortiGate unit should retry the health check if a health check fails. If all health checks, including retries, fail, the server is deemed unavailable. | 3 |
| timeout <seconds_int> | Enter the timeout in seconds. If the FortiGate unit does not receive a response to the health check in this period of time, the health check fails. | 2 |
| type {http ping tcp} | Select the protocol used by the health check monitor. | No default. |

local-in-policy, local-in-policy6

Use these commands to create firewall policies for traffic destined for the FortiGate unit itself.

Syntax

```
config firewall local-in-policy (for IPv4 traffic)
config firewall local-in-policy6 (for IPv6 traffic)
  edit <index_int>
    set action {accept | deny}
    set auto-asic-offload {enable | disable}
    set intf <name_str>
    set srcaddr <name_str>
    set dstaddr <name_str>
    set service <name_str>
    set schedule <name_str>
    set status {enable | disable}
  end
```

| Variable | Description | Default |
|---|---|-------------|
| <index_int> | Enter the unique ID number of this policy. Enter 0 to assign the next available ID. | |
| action {accept deny} | Select the action that the FortiGate unit will perform on traffic matching this firewall policy. | deny |
| auto-asic-offload {enable disable} | Enable or disable session offload to NP or SP processors. | enable |
| intf <name_str> | Enter the source interface. This is the interface through which the traffic reaches the FortiGate unit. | No default. |
| srcaddr <name_str> | Enter one or more source firewall addresses for the policy. Separate multiple firewall addresses with a space. | No default. |
| dstaddr <name_str> | Enter one or more destination firewall addresses for the policy. Separate multiple firewall addresses with a space. | No default. |
| service <name_str> | Enter the name of one or more services, or a service group, to match with the firewall policy. Separate multiple services with a space. | No default. |
| schedule <name_str> | Enter the name of the one-time or recurring schedule or schedule group to use for the policy. | No default. |
| status {enable disable} | Enable or disable this policy. | enable |

mms-profile

Use this command to configure MMS profiles. This command applies to FortiOS Carrier only.

Syntax

```
config firewall mms-profile
edit <profile_str>
    set avnotificationtable <index_int>
    set bwordtable <index_int>
    set carrier-endpoint-prefix {enable | disable}
    set carrier-endpoint-prefix-range-min <limit_int>
    set carrier-endpoint-prefix-range-max <limit_int>
    set carrier-endpoint-prefix-string <prefix_str>
    set carrierendpointbwltable <index_int>
    set comment <str>
    set exmwordtable <index_int>
    set filepattable <index_int>
    set mm1 {archive-full archive-summary avmonitor avquery
        bannedword block carrier-endpoint-bwl chunkedbypass
        clientcomfort exemptword no-content-summary oversize
        remove-blocked scan server-comfort}
    set mm1-addr-hdr <identifier_str>
    set mm1-addr-source {cookie | http-header}
    set mm1-convert-hex {enable | disable}
    set mm1-retr-dupe {enable | disable}
    set mm1-retrieve-scan {enable | disable}
    set mm1comfortamount <size_int>
    set mm1comfortinterval <seconds_int>
    set mm3 {archive-full archive-summary avmonitor avquery
        bannedword block carrier-endpoint-bwl fragmail
        no-content-summary oversize remove-blocked scan
        servercomfort splice}
    set mm4 {archive-full archive-summary avmonitor avquery
        bannedword block carrier-endpoint-bwl fragmail
        no-content-summary oversize remove-blocked scan
        servercomfort splice}
    set mm7 {archive-full archive-summary avmonitor avquery
        bannedword block carrier-endpoint-bwl chunkedbypass
        clientcomfort exemptword no-content-summary oversize
        remove-blocked scan server-comfort}
    set mm1oversizelimit <limit_int>
    set mm3oversizelimit <limit_int>
    set mm4oversizelimit <limit_int>
    set mm7-addr-hdr <identifier_str>
    set mm7-addr-source {cookie | http-header}
    set mm7-convert-hex {enable | disable}
    set mm7comfortamount <size_int>
    set mm7comfortinterval <seconds_int>
    set mm7oversizelimit <limit_int>
    set mms-checksum-table <tableID_int>
```

```
set mmsbwordthreshold <score_int>
config dupe {mm1 | mm4}
    set action1 {alert-notif archive archive-first block
        intercept log}
    set block-time1 <minutes_int>
    set limit1 <duplicatetrigger_int>
    get protocol1
    set status1 {enable | disable}
    set status2 {enable | disable}
    set window1 <minutes_int>
end
config flood {mm1 | mm4}
    set action1 {alert-notif archive archive-first block
        intercept log}
    set block-time1 <minutes_int>
    set limit1 <floodtrigger_int>
    set status1 {enable | disable}
    set status2 {enable | disable}
    set window1 <minutes_int>
end
config log
    set log-antispam-mass-mms {enable | disable}
    set log-av-block {enable | disable}
    set log-av-carrier-endpoint-filter {enable | disable}
    set log-av-oversize {enable | disable}
    set log-av-virus {enable | disable}
    set log-intercept {enable | disable}
    set log-mms-notification {enable | disable}
    set log-web-content {enable | disable}
end
config notification {alert-dupe-1 | alert-flood-1 | mm1 | mm3 |
    mm4 | mm7}
    set alert-int <int>
    set alert-int-mode {minutes | hours}
    set alert-src-msisdn <str>
    set alert-status {enable | disable}
    set bword-int <noticeinterval_int>
    set bword-int-mode {minutes | hours}
    set bword-status {enable | disable}
    set carrier-endpoint-bwl-int <interval_int>
    set carrier-endpoint-bwl-int-mode {hours | minutes}
    set carrier-endpoint-bwl-status {enable | disable}
    set days-allowed {monday tuesday wednesday thursday friday
        saturday sunday}
    set detect-server {enable | disable}
    set dupe-int <interval_int>
    set dupe-int-mode {hours | minutes}
    set dupe-status {enable | disable}
    set file-block-int <interval_int>
```

```

set file-block-int-mode {hours | minutes}
set file-block-status {enable | disable}
set flood-int <interval_int>
set flood-int-mode {hours | minutes}
set flood-status {enable | disable}
set from-in-header {enable | disable}
set mmsc-hostname {<fqdn_str> | <ipv4>}
set mmsc-password <passwd_str>
set mmsc-port <port_int>
set mmsc-url <url_str>
set mmsc-username <user_str>
set msg-protocol {mm1 | mm3 | mm4 | mm7}
set msg-type {deliver-req | send-req}
get protocol
set rate-limit <limit_int>
set tod-window-start <window_time>
set tod-window-duration <window_time>
set user-domain <fqdn_str>
set vas-id <vas_str>
set vasp-id <vasp_str>
set virus-int <interval_int>
set virus-int-mode {hours | minutes}
set virus-status {enable | disable}
end
config notif-msisdn
edit <msisdn_int>
    set threshold {dupe-thresh-1 dupe-thresh-2 dupe-thresh-3
        flood-thresh-1 flood-thresh-2 flood-thresh-3}
end
end
end

```

| Variable | Description | Default |
|---------------------------------------|---|-------------|
| <profile_str> | Enter the name of this MMS profile. | No default. |
| avnotificationtable <index_int> | Enter the ID number of the antivirus notification list to be used for the MMS profile. Antivirus notification tables contain virus names that, when detected, will have the FortiGate unit send a notification message to the administrator. For more information on antivirus notification tables, see “notification” on page 63 | No default. |
| bwordtable <index_int> | Enter the ID number of the web content block filter to be used for MMS traffic. The web content block tables can be configured using the <code>config webfilter bword</code> command. | No default. |
| carrierendpointbwtable <index_int> | Enter the ID number of the endpoint, such as MSISDN, filtering table to use for MMS traffic with the MMS profile. | No default. |

| Variable | Description | Default |
|---|--|-------------|
| carrier-endpoint-prefix { enable disable } | Select to add the country code to the extracted carrier endpoint, such as MSISDN, for logging and notification purposes. You can limit the number length for the test numbers used for internal monitoring without a country code. | disable |
| carrier-endpoint-prefix-range-min <limit_int> | Enter the minimum carrier endpoint prefix length. If this and endpoint-prefix-range-max are set to zero (0), length is not limited. This option appears only if msisdn-prefix is enable. | 0 |
| carrier-endpoint-prefix-range-max <limit_int> | Enter the maximum endpoint prefix length. If this and endpoint-prefix-range-min are set to zero (0), length is not limited. This option appears only if msisdn-prefix is enable. | 0 |
| carrier-endpoint-prefix-string <prefix_str> | Enter the endpoint, such as MSISDN, prefix. This option appears only if endpoint-prefix is enable. | No default. |
| comment <str> | Enter an optional comment to give additional detail about the MMS profile. | |
| exmwordtable <index_int> | Enter the ID number of the webfilter exempt word list to be used with the MMS profile. The web content exempt tables can be configured using the <code>config webfilter exmword</code> command. | No default. |
| filepattable <index_int> | Enter the ID number of the file pattern list to be used with the MMS profile. | 0 |

| Variable | Description | Default |
|--|--|------------------------------|
| mm1 { archive-full archive-summary avmonitor avquery bannedword block carrier-endpoint-bwl chunkedbypass clientcomfort exemptword no-content-summary oversize remove- blocked scan server-comfort } | <p>Select actions, if any, the FortiGate unit will take on MMS messages of the specified protocol.</p> <p>archive-full — Content archive both metadata and the MMS message itself.</p> <p>archive-summary — Content archive metadata.</p> <p>avmonitor — Log detected viruses, but allow them through the firewall without modification.</p> <p>avquery — Use the FortiGuard Antivirus service for virus detection using MD5 checksums.</p> <p>bannedword — Block messages containing content in the banned word list.</p> | No default. |
| mm3 { archive-full archive-summary avmonitor avquery bannedword block carrier-endpoint-bwl fragmail no-content-summary oversize remove- blocked scan servercomfort splice } | <p>block — Block messages matching the file patterns selected by <code>mms-file-pat-table</code>, even if the files do not contain viruses.</p> <p>carrier-endpoint-bwl — Enable the black/white list specified with the <code>carrierendpointbwltable</code> command.</p> <p>chunkedbypass — Allow web sites that use chunked encoding for HTTP to bypass the firewall. Chunked encoding means the HTTP message body is altered to allow it to be transferred in a series of chunks. Use of this feature is a risk. Malicious content could enter the network if web content is allowed to bypass the firewall. This option only available for the <code>mm1</code> and <code>mm7</code> commands.</p> | no-content-summary splice |
| mm4 { archive-full archive-summary avmonitor avquery bannedword block carrier-endpoint-bwl fragmail no-content-summary oversize remove- blocked scan servercomfort splice } | <p>clientcomfort — Apply client comforting to prevent client timeout. This option is available only for <code>mm1</code> and <code>mm7</code>.</p> <p>exemptword — Exempt words from content blocking. This option only available for the <code>mm1</code> and <code>mm7</code> commands.</p> | splice |
| mm7 { archive-full archive-summary avmonitor avquery bannedword block carrier-endpoint-bwl chunkedbypass clientcomfort exemptword no-content-summary oversize remove- blocked scan server-comfort } | <p>fragmail — Pass fragmented email messages. Fragmented email messages cannot be scanned for viruses. This option only available for the <code>mm3</code> and <code>mm4</code> commands.</p> <p>no-content-summary — Omit MMS filtering statistics from the dashboard.</p> <p>oversize — Block files that are over the file size limit.</p> <p>remove-blocked — Remove blocked items from messages.</p> <p>scan — Scan files for viruses and worms.</p> <p>server-comfort — Apply server comforting and prevent server timeout. This option is available only for <code>mm1</code> and <code>mm7</code>.</p> | No default. |

| Variable | Description | Default |
|--|--|-----------------------------------|
| | splice — Simultaneously scan a message and send it to the recipient. If the FortiGate unit detects a virus, it prematurely terminates the connection and returns an error message to the recipient, listing the virus name and infected file name. This option is available only for <code>mm3</code> and <code>mm4</code> . | |
| <code>mm1-addr-hdr</code> <identifier_str> | <p>Enter the sender address (MSISDN) identifier.</p> <p>If <code>mm1-addr-source</code> is <code>http-header</code>, the address and its identifier in the HTTP request header is in the format of:</p> <pre><Sender Address Identifier>: <MSISDN Value></pre> <p>For example, the HTTP header might contain:</p> <pre>x-up-calling-line-id: 6044301297</pre> <p>where <code>x-up-calling-line-id</code> would be the Sender Address Identifier.</p> <p>If <code>mm1-addr-source</code> is <code>cookie</code>, the address and its identifier in the HTTP request header's Cookie field is in the format of attribute-value pairs:</p> <pre>Cookie: id=<cookie-id>; <Sender Address Identifier>=<MSISDN Value></pre> <p>For example, the HTTP request headers might contain:</p> <pre>Cookie: id=0123jff!a;x-up-calling-line-id=6044301297</pre> <p>where <code>x-up-calling-line-id</code> would be the sender address identifier.</p> | <code>x-up-calling-line-id</code> |
| <code>mm1-addr-source</code> { <code>cookie</code> <code>http-header</code> } | Select to extract the sender's address from the HTTP header field or a cookie. | <code>http-header</code> |
| <code>mm1-convert-hex</code> { <code>enable</code> <code>disable</code> } | Select to convert the sender address from ASCII to hexadecimal or from hexadecimal to ASCII. This is required by some applications. | <code>disable</code> |
| <code>mm1-retr-dupe</code> { <code>enable</code> <code>disable</code> } | <p>Select to scan MM1 <code>mm1-retr</code> messages for duplicates. By default, <code>mm1-retr</code> messages are not scanned for duplicates as they may often be the same without necessarily being bulk or spam.</p> <p>This option is available only if <code>status</code> is <code>enable</code> for the <code>config dupe mm1</code> command.</p> | <code>disable</code> |
| <code>mm1-retrieve-scan</code> { <code>enable</code> <code>disable</code> } | Select to scan message retrieval by MM1. If you select <code>scan</code> for all MMS interfaces, messages are scanned while being sent, and so scanning message retrieval by MM1 is redundant. In this case, you can disable MM1 message retrieval scanning to improve performance. | <code>enable</code> |
| <code>mm1comfortamount</code> <size_int> | <p>Enter the number of bytes client comforting sends each interval to show a download is progressing.</p> <p>The interval time is set using <code>mm1comfortinterval</code>.</p> | <code>1</code> |

| Variable | Description | Default |
|---|--|----------------------|
| mm1comfortinterval <seconds_int> | Enter the time in seconds before client comforting starts after a download has begun. It is also the interval between subsequent client comforting sends. The amount of data sent each interval is set using mm1comfortamount. | 10 |
| mm1oversizelimit <limit_int> | Block files in MM1 streams that are over this file size limit in KB. | 10240 |
| mm3oversizelimit <limit_int> | Block files in MM3 streams that are over this file size limit in KB. | 10240 |
| mm4oversizelimit <limit_int> | Block files in MM4 streams that are over this file size limit in KB. | 10240 |
| mm7-addr-hdr <identifier_str> | Enter the sender address (MSISDN) identifier. If mm7-addr-source is http-header, the address and its identifier in the HTTP request header is in the format of: <Sender Address Identifier>: <MSISDN Value> For example, the HTTP header might contain: x-up-calling-line-id: 6044301297 where x-up-calling-line-id would be the Sender Address Identifier. If mm7-addr-source is cookie, the address and its identifier in the HTTP request header's Cookie field is in the format of attribute-value pairs: Cookie: id=<cookie-id>; <Sender Address Identifier>=<MSISDN Value> For example, the HTTP request headers might contain: Cookie: id=0123jff!a;x-up-calling-line-id=6044301297 where x-up-calling-line-id would be the sender address identifier. | x-up-calling-line-id |
| mm7-addr-source {cookie http-header} | Select to extract the sender's address from the HTTP header field or a cookie. | http-header |
| mm7-convert-hex {enable disable} | Select to convert the sender address from ASCII to hexadecimal or from hexadecimal to ASCII. This is required by some applications. | disable |
| mm7oversizelimit <limit_int> | Block files in MM7 streams that are over this file size limit in KB. | 10240 |
| mm7comfortamount <size_int> | Enter the number of bytes client comforting sends each interval to show a download is progressing. The interval time is set using mm7comfortinterval. | 1 |
| mm7comfortinterval <seconds_int> | Enter the time in seconds before client comforting starts after a download has begun. It is also the interval between subsequent client comforting sends. The amount of data sent each interval is set using mm7comfortamount. | 10 |

| Variable | Description | Default |
|---|---|---------|
| mms-checksum-table <tableID_int> | Enter the MMS content checksum table ID. | |
| mmsbwordthreshold <score_int> | Enter the maximum score an MMS message can have before being blocked. If the combined scores of the content block patterns appearing in an MMS message exceed the threshold value, the message will be blocked. | 10 |
| remove-blocked-const-length {enable disable} | Select to preserve the length of the MMS message when removing blocked content, such as viruses. | disable |

config dupe {mm1 | mm4}

Duplicate MMS messages can result from bulk MMS messages, MMS spam, attacks, or other issues.

You can use the `config dupe` subcommand to detect and act on MMS duplicate messages. Thresholds that define excessive duplicate messages and response actions are both configurable.

You can configure MMS duplicate message detection for MM1 messages using `config dupe mm1` and for MM4 messages using `config dupe mm4`.

There are four threshold settings each for mm1 and mm4. The integer at the end of each command indicates which threshold you are configuring. By default, only the first threshold is available for configuration. Enable status2 to gain access to the second threshold. Then enable status3 to gain access to the third threshold. Finally, enable status 4 to gain access to the fourth threshold. They must be enabled in sequence.

| Variable | Description | Default |
|---|---|--------------------------------------|
| action1 {alert-notif archive archive-first block intercept log} | <p>Select the actions to take, if any, when excessive duplicate messages are detected. To select more than one action, separate each action with a space.</p> <p>alert-notif — Enable to have the FortiGate unit send a notification message if this threshold is exceeded.</p> <p>archive — Archive duplicates in excess of the configured threshold.</p> <p>archive-first — Archive the first duplicate in excess of the configured threshold.</p> <p>block — Block and intercept excess duplicates. If block is selected, messages are also intercepted, even if <code>intercept</code> is not selected.</p> <p>intercept — Intercept excess duplicates.</p> <p>log — Log excess duplicates. This option takes effect only if logging is enabled for bulk MMS message detection. See “log-antispam-mass-mms {enable disable}” on page 158.</p> <p>This option appears only if <code>status</code> is set to <code>enable</code> for the MMS interface.</p> | archive block intercept log |
| block-time1 <minutes_int> | <p>Enter the amount of time in minutes during which the FortiGate unit will perform the <code>action</code> after a message flood is detected.</p> <p>This option appears only if <code>status</code> is <code>enable</code> for the MMS interface.</p> | 100 |
| limit1 <duplicate-trigger_int> | <p>Enter the number of messages which signifies excessive message duplicates if exceeded within the window.</p> <p>This option appears only if <code>status</code> is <code>enable</code> for the MMS interface.</p> | 100 |
| protocol1 | <p>The MMS interface that you are configuring. <code>protocol</code> can be <code>mm1</code> or <code>mm2</code> depending on whether you entered <code>config dupe mm1</code> or <code>config dupe mm4</code>.</p> <p>This variable can be viewed with the <code>get</code> command, but cannot be set.</p> | . |
| status1 {enable disable} | Select to detect and act upon duplicate MMS messages. | disable |
| status2 {enable disable} | Enable to gain access to the second set of threshold configuration settings. | disable |
| window1 <minutes_int> | <p>Enter the period of time in minutes during which excessive message duplicates will be detected if the <code>limit</code> is exceeded.</p> <p>This option appears only if <code>status</code> is <code>enable</code> for the protocol (MM1 or MM4).</p> | 60 |

config flood {mm1 | mm4}

Excessive MMS activity (message floods) can result from bulk MMS messages, MMS spam, attacks, or other issues.

You can use the `config flood` subcommand to detect and act on MMS message floods. Thresholds that define a flood of message activity and response actions are both configurable.

You can configure MMS flood detection for MM1 messages using `config flood mm1` and for MM4 messages using `config flood mm4`.

There are four threshold settings for mm1 and mm4. The integer at the end of each command indicates which threshold you are configuring. By default, only the first threshold is available for configuration. Enable `status2` to gain access to the second threshold. Then enable `status3` to gain access to the third threshold. Finally, enable `status 4` to gain access to the fourth threshold. They must be enabled in sequence.

| Variable | Description | Default |
|---|---|---------------------------|
| action1 {alert-notif archive archive-first block intercept log} | <p>Select which actions to take, if any, when excessive message activity is detected. To select more than one action, separate each action with a space.</p> <p>alert-notif — Enable to have the FortiGate unit send a notification message If this threshold is exceeded.</p> <p>archive — Archive messages in excess of the configured threshold.</p> <p>archive-first — Archive the first message in excess of the configured threshold.</p> <p>block — Block and intercept excess messages. If block is selected, messages are also intercepted, even if <code>intercept</code> is not selected.</p> <p>intercept — Intercept excess messages.</p> <p>log — Log excess messages. This option takes effect only if logging is enabled for bulk MMS message detection. See “log-antispam-mass-mms {enable disable}” on page 158.</p> <p>This option appears only if <code>status</code> is <code>enable</code> for the MMS interface.</p> | block intercept log |
| block-time1 <minutes_int> | <p>Enter the amount of time in minutes during which the FortiGate unit will perform the <code>action</code> after a message flood is detected.</p> <p>This option appears only if <code>status</code> is <code>enable</code> for the MMS interface.</p> | 100 |
| limit1 <floodtrigger_int> | <p>Enter the number of messages which signifies excessive message activity if exceeded within the <code>window</code>.</p> <p>This option appears only if <code>status</code> is <code>enable</code> for the MMS interface.</p> | 100 |
| protocol1 | <p>The MMS interface that you are configuring. <code>protocol</code> can be <code>mm1</code> or <code>mm2</code> depending on whether you entered <code>config flood mm1</code> or <code>config flood mm4</code>.</p> <p>This variable can be viewed with the <code>get</code> command, but cannot be <code>set</code>.</p> | |
| status1 {enable disable} | Select to detect and act upon excessive MMS message activity. | disable |

| Variable | Description | Default |
|---------------------------------|--|---------|
| status2 { enable disable } | Enable to gain access to the second threshold configuration settings. | disable |
| window1 <minutes_int> | Enter the period of time in minutes during which excessive message activity will be detected if the <code>limit</code> is exceeded. This option appears only if <code>status</code> is <code>enable</code> for the MMS interface. | 60 |

config log

Use this command to write event log messages when the options that you have enabled in this MMS profile perform an action. For example, if you enable antivirus protection you could also use the `config log` command to enable `log-av-block` so that the FortiGate unit writes an event log message every time a virus is detected.

All of the `config log` fields are the same as the corresponding `config policy` fields except the following

| Variable | Description | Default |
|--|---|---------|
| log-antispam-mass-mms { enable disable } | Enable to log duplicate or flood MMS notification messages. Also select the <code>log</code> action for each protocol and bulk MMS message event that you want to log. For details, see “action1 {alert-notif archive archive-first block intercept log}” on page 156 and “action1 {alert-notif archive archive-first block intercept log}” on page 156 . | disable |
| log-av-block { enable disable } | Enable to log blocked viruses and files. | disable |
| log-av-carrier-endpoint-filter { enable disable } | Enable to log endpoint, such as MSISDN, blocking, intercepts, and archiving in MMS messages. | disable |
| log-av-oversize { enable disable } | Enable to log oversized messages. | disable |
| log-av-virus { enable disable } | Enable to log detected viruses. | disable |
| log-intercept { enable disable } | Enable to log MMS intercept actions in MMS messages. | disable |
| log-mms-notification { enable disable } | Enable to log MMS notification messages in MMS messages. | disable |
| log-web-content { enable disable } | Enable to log blocked web content. | disable |

config notification {alert-dupe-1 | alert-flood-1 | mm1 | mm3 | mm4 | mm7}

Use this command to configure how the FortiGate unit sends MMS messages to MMS clients to inform them that messages have been sent from their device that violate the settings in this MMS profile. To enable sending notifications you need to enable notification types. You can enable all notification types or you can enable separate notifications for web content blocking, file blocking, end point blocking, flooding, duplicate messages, and virus scanning. You can also use the MMS notifications options to configure how the notification messages are sent.

The FortiGate unit sends notification messages immediately for the first event, then at a configurable interval if events continue to occur. If the interval does not coincide with the window of time during which notices may be sent, the FortiGate unit waits and sends the notice in the next available window. Subsequent notices contain a count of the number of events that have occurred since the previous notification.

There are separate notifications for each notification type, including virus events. Virus event notifications include the virus name. Up to three viruses are tracked for each user at a time. If a fourth virus is found, one of the existing tracked viruses is removed.

The notifications are MM1 `m-send-req` messages sent from the FortiGate unit directly to the MMSC for delivery to the client. The host name of the MMSC, the URL to which `m-send-req` messages are sent, and the port must be specified.

| Variable | Description | Default |
|---|--|--|
| alert-int <int> | Enter the interval the FortiGate will use to send alert messages. The integer you enter will be interpreted as hours or minutes depending on how the <code>alert-int-mode</code> command is set. | 1 |
| alert-int-mode {minutes hours} | Enter <code>minutes</code> or <code>hours</code> . This setting will determine whether the integer entered with the <code>alert-int</code> command is interpreted as minutes or hours. | hour |
| alert-src-msisdn <str> | Enter the address the alert messages will appear to be sent from. | |
| alert-status {enable disable} | Enable to have the FortiGate unit send alert messages. | enable |
| bword-int <noticeinterval_int> | Enter the banned word notification send interval. | 24 |
| bword-int-mode {minutes hours} | Select whether the value specified in the <code>bword-int</code> command is minutes or hours. | hours |
| bword-status {enable disable} | Select to send notices for banned word events. | disable |
| carrier-endpoint-bwl-int <interval_int> | Enter the amount of time between notifications for endpoint black/white list events. Also set <code>endpoint-bwl-status</code> to <code>enable</code> and select the time unit in <code>endpoint-bwl-int-mode</code> . | 24 |
| carrier-endpoint-bwl-int-mode {hours minutes} | Select the unit of time in minutes or hours for <code>carrier-endpoint-bwl-int</code> . | hours |
| carrier-endpoint-bwl-status {enable disable} | Select to send notices for endpoint black/white list events. | disable |
| days-allowed {monday tuesday wednesday thursday friday saturday sunday} | Notifications will be sent on the selected days of the week. | monday tuesday wednesday thursday friday saturday sunday |
| detect-server {enable disable} | Select to automatically determine the server address. | enable |
| dupe-int <interval_int> | Enter the amount of time between notifications of excessive MMS duplicates. Also set <code>dupe-status</code> to <code>enable</code> and select the time unit in <code>dupe-int-mode</code> . | 24 |
| dupe-int-mode {hours minutes} | Select the unit of time in minutes or hours for <code>dupe-int</code> . Available only for MM1 and MM4 notifications. | hours |

| Variable | Description | Default |
|---------------------------------------|---|--|
| dupe-status {enable disable} | Select to send notices for excessive MMS message duplicate events. Available only for MM1 and MM4 notifications. Available only for MM1 and MM4 notifications. | disable |
| file-block-int <interval_int> | Enter the amount of time between notifications of file block events. Also set <code>file-block-status</code> to <code>enable</code> and select the time unit in <code>file-block-int-mode</code> . | 24 |
| file-block-int-mode {hours minutes} | Select whether the value specified in the <code>file-block-int</code> command is minutes or hours. | hours |
| file-block-status {enable disable} | Select to send notices for file block events. | disable |
| flood-int <interval_int> | Enter the amount of time between notifications of excessive MMS activity. Also set <code>flood-status</code> to <code>enable</code> and select the time unit in <code>flood-int-mode</code> . Available only for MM1 and MM4 notifications. | 24 |
| flood-int-mode {hours minutes} | Select the unit of time in minutes or hours for <code>flood-int</code> . Available only for MM1 and MM4 notifications. | hours |
| flood-status {enable disable} | Select to send notices for excessive MMS message activity events. Available only for MM1 and MM4 notifications. | disable |
| from-in-header {enable disable} | Select to insert the “from” address in the HTTP header. | disable |
| mmsc-hostname {<fqdn_str> <ipv4>} | Enter the FQDN or the IP address of the destination server. | No default. |
| mmsc-password <passwd_str> | Enter the password required for sending messages using this server. (Optional) | No default. |
| mmsc-port <port_int> | Enter the port number the server is using. | Varies by msg-protocol. |
| mmsc-url <url_str> | Enter the URL address of the server. | No default. |
| mmsc-username <user_str> | Enter the user-name required for sending messages using this server. (Optional) | No default. |
| msg-protocol {mm1 mm3 mm4 mm7} | Select the protocol to use for sending notification messages. | Depends on protocol {mm1 mm3 mm4 mm7}. |
| msg-type {deliver-req send-req} | Select the type of notification message directed to either a VASP or a MMSC. | deliver-req |

| Variable | Description | Default |
|--------------------------------------|--|-------------|
| protocol | The MMS interface that you are configuring. <code>protocol</code> can be <code>mm1</code> , <code>mm3</code> , <code>mm4</code> or <code>mm7</code> depending on the message type that you are configuring notifications for. This variable can be viewed with the <code>get</code> command, but cannot be <code>set</code> . | |
| rate-limit <limit_int> | Enter the number of notifications to send per second. If you enter zero (0), the notification rate is not limited. | 0 |
| tod-window-start <window_time> | Select the time of day to begin sending notifications. If you select a start and end time of zero (00 : 00), notifications are not limited by time of day. | 00:00 |
| tod-window-duration <window_time> | Select the duration of the period during which the FortiGate unit will send notification messages. If you select a start and duration time of zero (00 : 00), notifications are not limited by time of day. | 00:00 |
| user-domain <fqdn_str> | Enter the FQDN of the server to which the user's address belongs. | No default. |
| vas-id <vas_str> | Enter the value added service (VAS) ID to be used when sending a notification message. This option is available only when <code>msg-type</code> is set to <code>send-req</code> . | No default. |
| vasp-id <vasp_str> | Enter the value added service provider (VASP) ID to be used when sending a notification message. This option is available only when <code>msg-type</code> is set to <code>send-req</code> . | No default. |
| virus-int <interval_int> | Enter the amount of time between notifications for antivirus events. Also set <code>virus-status</code> to <code>enable</code> and select the time unit in <code>virus-int-mode</code> . | 24 |
| virus-int-mode {hours minutes} | Select the unit of time in minutes or hours for <code>virus-int</code> . | hours |
| virus-status {enable disable} | Select to send notices for antivirus events. | disable |

Example

This example shows how to enable sending MMS notifications for all MM3 notification types and set the interval for each one to 400 minutes:

```
config firewall mms-profile
  edit example
    config notification mm3
      set bword-status enable
      set bword-int-mode minutes
      set bword-int 400
      set file-block-status enable
      set file-block-mode minutes
      set file-block-int 400
      set carrier-endpoint-bwl-status enable
      set carrier-endpoint-bwl-int-mode minutes
      set carrier-endpoint-bwl-int 400
      set virus-status enable
      set virus-int-mode minutes
      set virus-int 400
    end
  end
```

config notif-msisdn

Individual MSISDN users can be configured to have specific duplicate and flood thresholds.

| Variable | Description | Default |
|--|---|---------|
| <msisdn_int> | Enter the MSISDN number. Enter a new number to create a new entry. | |
| threshold {dupe-thresh-1 dupe-thresh-2 dupe-thresh-3 flood-thresh-1 flood-thresh-2 flood-thresh-3} | Enter the thresholds on which this MSISDN user will receive an alert. Clear all thresholds with the <code>unset threshold</code> command. | (null) |

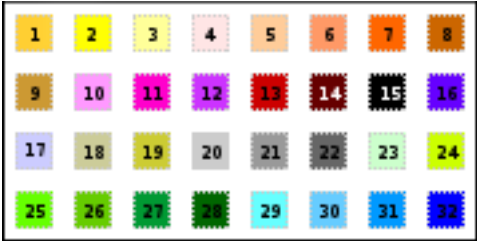
multicast-address

Use this command to configure multicast firewall addresses used in firewall multicast policies.

Addresses, address groups, and virtual IPs must have unique names to avoid confusion in firewall policies. If an address is selected in a policy, it cannot be deleted until it is deselected from the policy.

Syntax

```
config firewall multicast-address
edit <name_str>
    set associated-interface <interface_str>
    set color <color_int>
    set comment <comment_string>
    set end-ip <address_ipv4>
    set start-ip <address_ipv4>
    set subnet <ip4mask>
    set tags <tags_str>
    set type {broadcastmask | multicastrange}
    set visibility {enable | disable}
end
```

| Variable | Description | Default |
|---|---|-----------------|
| <name_str> | Enter the name of the address. There are also predefined addresses: Bonjour, EIGRP, OSPF, all_hosts, all_routers. | No default. |
| associated-interface <interface_str> | Enter the name of the associated interface. If not configured, the firewall address is bound to an interface during firewall policy configuration. | No default. |
| color <color_int> | Set the icon color to use in the web-based manager. 0 sets the default, color 1.  | 0 |
| comment <comment_string> | Enter a descriptive comment for this address. | No default. |
| end-ip <address_ipv4> | If type is iprange, enter the last IP address in the range. | 0.0.0.0 |
| start-ip <address_ipv4> | If type is iprange, enter the first IP address in the range. | 0.0.0.0 |
| subnet <ip4mask> | Enter a broadcast IP/mask to be treated as multicast address. Available when type is broadcastmask. | 0.0.0.0 0.0.0.0 |
| tags <tags_str> | Enter object tags applied to this address. Separate tag names with spaces. | null |

| Variable | Description | Default |
|---|---|----------------|
| type {broadcastmask multicastrange} | Select the type of multicast address: broadcastmask—define a broadcast IP/mask in subnet to be treated as multicast address. multicastrange—define multicast IP address range in start-ip and end-ip. | multicastrange |
| visibility {enable disable} | Select whether this address is available in firewall multicast policy address fields in the web-based manager. | enable |

multicast-policy

Use this command to configure a source NAT IP. This command can also be used in Transparent mode to enable multicast forwarding by adding a multicast policy.

The matched forwarded (outgoing) IP multicast source IP address is translated to the configured IP address. For additional options related to multicast, see [multicast-forward {enable | disable}](#) in “system settings” on page 670 and [tp-mc-skip-policy {enable | disable}](#) in “system global” on page 523.

Syntax

```
config firewall multicast-policy
edit <index_int>
    set action {accept | deny}
    set auto-asic-offload {enable | disable}
    set dnat <address_ipv4>
    set dstaddr <addr_name_list>
    set dstintf <name_str>
    set logtraffic {enable | disable}
    set snat {enable | disable}
    set srcaddr <addr_name_list>
    set srcintf <name_str>
    set status {enable | disable}
    set protocol <multicastlimit_int>
    set start-port <port_int>
    set end-port <port_int>
end
```

| Variable | Description | Default |
|--------------------------------------|--|-------------|
| <index_int> | Enter the unique ID number of this multicast policy. | No default. |
| action {accept deny} | Enter the policy action. | accept |
| auto-asic-offload {enable disable} | Enable or disable session offloading to SP processors. Only available in NAT/Route operation mode. | enable |
| dnat <address_ipv4> | Enter an IP address to destination network address translate (DNAT) externally received multicast destination addresses to addresses that conform to your organization's internal addressing policy. | 0.0.0.0 |
| dstaddr <addr_name_list> | Enter the names of multicast destination addresses for this policy. Separate address names with spaces. These addresses are defined in firewall multicast-address . | No default. |
| dstintf <name_str> | Enter the destination interface name to match against multicast NAT packets. | No default. |
| logtraffic {enable disable} | Enable or disable recording traffic log messages for this policy. | disable |
| snat {enable disable} | Enable substitution of outgoing interface IP address for the original source IP address. | disable |
| srcaddr <addr_name_list> | Enter the names of source IP addresses for this policy. Separate address names with spaces. These addresses are defined in firewall address , address6 . | No default. |

| Variable | Description | Default |
|----------------------------------|---|-------------|
| srcintf <name_str> | Enter the source interface name to match against multicast NAT packets. | No default. |
| status {enable disable} | Enable or disable this policy. | enable |
| protocol <multicastlimit_int> | Limit the number of protocols (services) sent out via multicast using the FortiGate unit. | 0 |
| start-port <port_int> | The beginning of the port range used for multicast. Availability of this field depends on protocol. | No default. |
| end-port <port_int> | The end of the port range used for multicast. Availability of this field depends on protocol. | 65535 |

policy, policy6

Use these commands to add, edit, or delete firewall policies.

- Use `config firewall policy` for IPv4 policies
- Use `config firewall policy6` for IPv6 policies

Firewall policies control all traffic passing through the FortiGate unit. Firewall policies are instructions used by the FortiGate unit to decide what to do with a connection request. The policy directs the firewall to allow the connection, deny the connection, require authentication before the connection is allowed, or apply IPsec or SSL VPN processing.



If you are creating a policy that involves IPv6 addresses, some of the IPv4 options, such as NAT and VPN settings, are not applicable.

Syntax

```
config firewall policy or config firewall policy6
edit <index_int>
    set action {accept | deny | ipsec | ssl-vpn}
    set active-auth-method {basic | digest | form | ntlm}
    set application {enable | disable}
    set application-list <name_str>
    set auth-cert <certificate_str>
    set auth-path {enable | disable}
    set auth-portal {enable | disable}
    set auth-redirect-addr <domainname_str>
    set auto-asic-offload {enable | disable}
    set av-profile <name_str>
    set bandwidth {enable | disable}
    set capture-packet {enable | disable}
    set central-nat {enable | disable}
    set client-reputation {enable | disable}
    set client-reputation-mode {learning | monitoring}
    set comments <comment_str>
    set custom-log-fields <fieldid_int>
    set deep-inspection-options <profile_name>
    set device-detection-portal {enable | disable}
    set diffserv-forward {enable | disable}
    set diffserv-reverse {enable | disable}
    set diffservcode-forward <dscp_bin>
    set diffservcode-rev <dscp_bin>
    set disclaimer {enable | disable}
    set dlp-sensor <name_str>
    set dponly {enable | disable}
    set dstaddr <name_str>
    set dstaddr6 <name_str>
    set dstaddr-negate {enable | disable}
```

```
set dstintf <name_str>
set email-collection-portal {enable | disable}
set endpoint-check {enable | disable}
set endpoint-keepalive-interface <intf_name>
set endpoint-profile <ep_profile_name>
set failed-connection {enable | disable}
set fall-through-unauthenticated {enable | disable}
set firewall-session-dirty {check-all | check-new}
set fixedport {enable | disable}
set forticlient-compliance-devices <device_type_str>
set forticlient-compliance-enforcement-portal
    {enable | disable}
set fsso {enable | disable}
set fsso-server-for-ntlm <server_str>
set geo-location {enable | disable}
set global-label <label_str>
set gtp_profile <name_str>
set icap-profile <icap_pr_name>
set identity-based {enable | disable}
set identity-based-route <idroute_name>
set identity-from {auth | device}
set inbound {enable | disable}
set ip-based {enable | disable}
set ippool {enable | disable}
set ips-sensor <name_str>
set label <label_string>
set logtraffic {all | utm | disable}
set logtraffic-app {enable | disable}
set logtraffic-start {enable | disable}
set log-unmatched-traffic {disable | enable}
set match-vip {enable | disable}
set mms-profile <name_str>
set nat {enable | disable}
set natinbound {enable | disable}
set natip <address_ipv4mask>
set natoutbound {enable | disable}
set netscan-discover-hosts {enable | disable}
set ntlm {enable | disable}
set ntlm-enabled-browsers <user-agent_string>
set ntlm-guest {enable | disable}
set outbound {enable | disable}
set per-ip-shaper <shaper_name>
set permit-any-host {enable | disable}
set permit-stun-host {enable | disable}
set poolname <name_str>
set profile-type {group | single}
set profile-group <name_str>
set profile-protocol-options <name_str>
```



```
set redirect-url <name_str>
set replacemsg-group <name_str>
set replacemsg-override-group <group_string>
set require-tfa {enable | disable}
set rso {enable | disable}
set rtp-nat {disable | enable}
set rtp-addr <name_str>
set schedule <name_str>
set schedule-timeout {enable | disable}
set send-deny-packet {enable | disable}
set service <name_str>
set service-negate {enable | disable}
set sessions {enable | disable}
set session-ttl <session_time_int>
set spamfilter-profile <name_str>
set srcaddr <name_str>
set srcaddr6 <name_str>
set srcaddr-negate {enable | disable}
set srcintf <name_str>
set sslvpn-auth {any | ldap | local | radius | tacacs+}
set sslvpn-ccert {enable | disable}
set sslvpn-cipher {any | medium | high}
set sso-auth-method {fsso | rso}
set status {enable | disable}
set tags <tags_str>
set tcp-mss-sender <maximumsize_int>
set tcp-mss-receiver <maximumsize_int>
set timeout-send-rst {enable | disable}
set traffic-shaper <name_str>
set traffic-shaper-reverse <name_str>
set utm-status {disable | enable}
set voip-profile <name_str>
set vpntunnel <name_str>
set wanopt {enable | disable}
set wanopt-detection {active | passive | off}
set wanopt-profile <name_str>
set wanopt-peer <peer_name>
set wccp {enable | disable}
set web-auth-cookie {enable | disable}
set webcache {disable | enable}
set webcache-https {disable | any | ssl-server}
set webfilter-profile <name_str>
set webproxy-forward-server <fwd_srv_name_string>
set wso {enable | disable}
```

```
config identity-based-policy
  edit <policy_id>
    set action {accept | deny | capture}
    set application-list <name_str>
    set av-profile <name_str>
    set captive-portal {device-identification
      | email-collection | forticlient-download}
    set client-reputation {enable | disable}
    set deep-inspection-options <profile_name>
    set devices <device_list>
    set dlp-sensor <name_str>
    set dstaddr <name_str>
    set endpoint-compliance {enable | disable}
    set groups <group_name>
    set ips-sensor <name_str>
    set logtraffic {enable | disable}
    set mms-profile <name_str>
    set per-ip-shaper <name_str>
    set profile-group {group | single}
    set profile-protocol-options <name_str>
    set profile-type {group | single}
    set schedule <name_str>
    set service <name_str>
    set spamfilter-profile <name_str>
    set sslvpn-realm <realm-url-path>
    set sslvpn-realm <realm-url-path>
    set traffic-shaper <name_str>
    set traffic-shaper-reverse <name_str>
    set users <user_name_list>
    set utm-status {disable | enable}
    set voip-profile <name_str>
    set webfilter-profile <name_str>
  end
end
end
```

| Variable | Description | Default |
|---|--|-------------|
| <index_int> | Enter the unique ID number of this policy. | No default. |
| action {accept deny ipsec ssl-vpn} | <p>Select the action that the FortiGate unit will perform on traffic matching this firewall policy.</p> <p>accept — Allow packets that match the firewall policy. Also enable or disable <code>nat</code> to make this a NAT policy (NAT/Route mode only), enable or disable <code>ippool</code> so that the NAT policy selects a source address for packets from a pool of IP addresses added to the destination interface, and enable or disable <code>fixedport</code> so that the NAT policy does not translate the packet source port.</p> <p>deny — Deny packets that match the firewall policy.</p> <p>ipsec — Allow and apply IPSec VPN. When <code>action</code> is set to <code>ipsec</code>, you must specify the <code>vpntunnel</code> attribute. You may also enable or disable the <code>inbound</code>, <code>outbound</code>, <code>natoutbound</code>, and <code>natinbound</code> attributes and/or specify a <code>natip</code> value.</p> <p>ssl-vpn — Allow and apply SSL VPN. When <code>action</code> is set to <code>ssl-vpn</code>, you may specify values for the <code>sslvpn-auth</code>, <code>sslvpn-ccert</code>, and <code>sslvpn-cipher</code> attributes.</p> <p>For IPv6 policies, only <code>accept</code>, <code>deny</code> and <code>ssl-vpn</code> options are available.</p> | deny |
| active-auth-method {basic digest form ntlm} | <p>Select the active authentication method to use. This is available if <code>srcintf</code> is <code>web-proxy</code> and <code>identity-based</code> is enabled. If <code>sso-auth-method</code> is set, it is tried first.</p> <p>basic — client must authenticate with a user-ID and password for each realm. User name and password are sent unencrypted</p> <p>digest — a nonce value is sent to client in the challenge and is included when the client sends a response of an MD5 checksum for the combination of their user-ID, password, nonce, and URI requested. The FortiOS unit has all this information and can confirm the MD5 checksum is correct.</p> <p>fssso — use Fortinet Single Sign On (FSSO) authentication with FSSO clients on a Windows AD network. This option is available only if <code>ip-based</code> is enabled.</p> <p>form — use Form-based authentication</p> <p>ntlm — NT Lan manager (ntlm) - ntlm uses Windows AD and Internet Explorer to authenticate through the browser. Useful when FSSO client cannot be installed on Windows AD server.</p> <p>If <code>basic</code> is enabled, <code>FSSO_GUEST_user</code> cannot be selected under Identity Based Policy (IBP).</p> | null |

| Variable | Description | Default |
|---|---|-------------|
| application {enable disable} | Enable or disable tracking the application usage of each host. This is available when <code>auto-profiling</code> is enabled. | disable |
| application-list <name_str> | Enter the name of the application list to add to the firewall policy. This option appears only if <code>identity-based</code> is <code>disable</code> and <code>utm-status</code> is <code>enable</code> . | (null) |
| auth-cert <certificate_str> | Select an HTTPS server certificate for policy authentication. <code>self-sign</code> is the built-in, self-signed certificate; if you have added other certificates, you may select them instead. This option appears only if <code>identity-based</code> is <code>enable</code> . | No default. |
| auth-path {enable disable} | Select to apply authentication-based routing. You must also specify a RADIUS server, and the RADIUS server must be configured to supply the name of an object specified in <code>config router auth-path</code> . For details on configuring authentication-based routes, see “router auth-path” on page 345 . This option appears only when the FortiGate unit is operating in NAT mode and <code>identity-based</code> is <code>enable</code> . For details on NAT and transparent mode, see “opmode {nat transparent}” on page 674 . | disable |
| auth-portal {enable disable} | Enable or disable use of the external authentication portal defined in firewall auth-portal . | disable |
| auth-redirect-addr <domainname_str> | Enter the IP address or domain name to redirect user HTTP requests after accepting the authentication disclaimer. The redirect URL could be to a web page with extra information (for example, terms of usage). To prevent web browser security warnings, this should match the CN field of the specified <code>auth-cert</code> , which is usually a fully qualified domain name (FQDN). This option appears only if <code>identity-based</code> is <code>enable</code> . | No default. |
| auto-asic-offload {enable disable} | Enable or disable session offload to NP or SP processors. This is available on models that have network processors. | enable |
| av-profile <name_str> | Enter the name of the antivirus profile to add to the firewall policy. This option appears only if <code>identity-based</code> is <code>disable</code> and <code>utm-status</code> is <code>enable</code> . To add an <code>av-profile</code> , you must obtain an adequate profile name in <code>profile-protection-options</code> . | (null) |

| Variable | Description | Default |
|---|--|-------------|
| bandwidth {enable disable} | Enable or disable tracking the bandwidth usage of each host. This is available when <code>auto-profiling</code> is enabled. | disable |
| block-notification {enable disable} | Enable to display Fortinet Bar in browser when a site is blocked. Fortinet Bar must be enabled in firewall profile-protocol-options . | disable |
| capture-packet {enable disable} | Enable or disable packet capture. This is available when <code>logtraffic</code> is <code>all</code> or <code>utm</code> . | disable |
| central-nat {enable disable} | Enable or disable use of the central NAT table in this policy. This is available only when <code>nat</code> is enabled. | disable |
| client-reputation {enable disable} | Enable to turn on client reputation monitoring. This option is visible only when <code>action</code> is set to <code>accept</code> . | disable |
| client-reputation-mode {learning monitoring} | Set client reputation mode to one of <code>learning</code> or <code>monitoring</code> . Set to <code>learning</code> to establish a baseline of client network usage patterns. Set to <code>monitoring</code> when baseline has been established. It will monitor the client's network patterns for abnormalities. When monitoring, client network usage data is logged for use in reports. This is available when <code>client-reputation</code> is enabled. | |
| comments <comment_str> | Enter a description or other information about the policy. (Optional) <code>comment_str</code> is limited to 63 characters. Enclose the string in single quotes to enter special characters or spaces. | No default. |
| custom-log-fields <fieldid_int> | Enter custom log field index numbers to append one or more custom log fields to the log message for this policy. Separate multiple log custom log field indices with a space. (Optional.) This option takes effect only if logging is enabled for the policy, and requires that you first define custom log fields. For details, see “log custom-field” on page 278 . | No default. |
| deep-inspection-options <profile_name> | Enter the name of the deep inspection options profile to apply. See “firewall deep-inspection-options” on page 109 . | No default. |
| device-detection-portal {enable disable} | Enable or disable the Device Detection Portal. | disable |
| diffserv-forward {enable disable} | Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic. If enabled, also configure <code>diffservcode-forward</code> . | disable |
| diffserv-reverse {enable disable} | Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of reverse (reply) traffic. If enabled, also configure <code>diffservcode-rev</code> . | disable |

| Variable | Description | Default |
|---|--|-------------|
| diffservcode-forward <dscp_bin> | <p>Enter the differentiated services code point (DSCP) value that the FortiGate unit will apply to the field of originating (forward) packets. The value is 6 bits binary. The valid range is 000000-111111.</p> <p>This option appears only if <code>diffserv-forward</code> is enable.</p> <p>For details and DSCP configuration examples, see the Knowledge Center article Differentiated Services Code Point (DSCP) behavior.</p> | 000000 |
| diffservcode-rev <dscp_bin> | <p>Enter the differentiated services code point (DSCP) value that the FortiGate unit will apply to the field of reply (reverse) packets. The value is 6 bits binary. The valid range is 000000-111111.</p> <p>This option appears only if <code>diffserv-rev</code> is enable</p> <p>For details and DSCP configuration examples, see the Knowledge Center article Differentiated Services Code Point (DSCP) behavior.</p> | 000000 |
| disclaimer {enable disable} | <p>Enable to display the authentication disclaimer page, which is configured with other replacement messages. The user must accept the disclaimer to connect to the destination.</p> | disable |
| dlp-sensor <name_str> | <p>Enter the name of the DLP sensor to add to the firewall policy.</p> <p>This option appears only if <code>identity-based</code> is disable and <code>utm-status</code> is enable.</p> | (null) |
| dponly {enable disable} | <p>For FortiOS Carrier, enable to configure the firewall policy to only accept sessions with source addresses that are in the dynamic profile user context list. Sessions with source addresses that are not in the user context list do not match the policy. For sessions that don't match the policy, the FortiOS Carrier unit continues searching down the policy list for a match.</p> | disable |
| dstaddr <name_str> dstaddr6 <name_str> | <p>Enter one or more destination firewall addresses, or a virtual IP, if creating a NAT policy. Separate multiple firewall addresses with a space.</p> <p>Use <code>dstaddr6</code> for IPv6 addresses.</p> <p>If <code>action</code> is set to <code>ipsec</code>, enter the name of the IP address to which IP packets may be delivered at the remote end of the IPsec VPN tunnel.</p> <p>If <code>action</code> is set to <code>ssl-vpn</code>, enter the name of the IP address that corresponds to the host, server, or network that remote clients need to access behind the FortiGate unit.</p> <p>For details on configuring virtual IPs, see “vip” on page 222.</p> | No default. |
| dstaddr-negate {enable disable} | <p>Enable to negate <code>dstaddr</code> match. This causes <code>dstaddr</code> to specify what the destination address must not be.</p> | disable |

| Variable | Description | Default |
|--|---|-------------|
| dstintf <name_str> | <p>Enter the destination interface(s) for the policy. Enter the source interface(s) for the policy. Separate interface names with spaces.</p> <p>The interface can be a physical interface, a VLAN subinterface, or a zone.</p> <p>If <code>action</code> is set to <code>ipsec</code>, enter the name of the interface to the external (public) network.</p> <p>If <code>action</code> is set to <code>ssl-vpn</code>, enter the name of the interface to the local (private) network.</p> <p>Note: If a interface or VLAN subinterface has been added to a zone, the interface or VLAN subinterface cannot be used for <code>dstintf</code>.</p> | No default. |
| email-collection-portal {enable disable} | Enable or disable email collection from new devices. | disable |
| endpoint-check {enable disable} | <p>Enable to perform endpoint NAC compliance check. This check denies access to this firewall policy for hosts that do not have up-to-date FortiClient Endpoint Security software running. You need to also configure <code>endpoint-profile</code>.</p> <p>Note: If the firewall policy involves a load balancing virtual IP, the endpoint compliance check is not performed.</p> <p>For more information, see “endpoint-control” on page 91.</p> | disable |
| endpoint-keepalive-interface <intf_name> | If endpoint-check is enabled, this field is available to specify the keepalive interface. The default is a null string, which is interpreted as the source interface. | null |
| endpoint-profile <ep_profile_name> | Select the endpoint NAC profile to apply. This is available when <code>endpoint-check</code> is enabled. For information about creating endpoint NAC profiles, see “endpoint-control profile” on page 93 . | No default. |
| failed-connection {enable disable} | Enable or disable tracking of failed connection attempts. This is available when <code>auto-profiling</code> is enabled. | disable |
| fall-through-unauthenticated {enable disable} | Enable to allow an unauthenticated user to skip authentication rules and possibly match another policy. | disable |
| firewall-session-dirty {check-all check-new} | <p>Select how to manage changes to a firewall policy:</p> <p><code>check-all</code> — flush all current sessions and re-evaluate them</p> <p><code>check-new</code> — keep existing sessions and apply policy change to new sessions only</p> | check-all |

| Variable | Description | Default |
|---|---|-------------|
| fixedport {enable disable} | Enable to preserve packets' source port number, which may otherwise be changed by a NAT policy. Some applications do not function correctly if the source port number is changed, and may require this option. If <code>fixedport</code> is <code>enable</code> , you should usually also enable IP pools; if you do not configure an IP pool for the policy, only one connection can occur at a time for this port. | disable |
| forticlient-compliance-devices <device_type_str> | Restrict the device types to which FortiClient enforcement applies. You can enter a space-delimited list containing any of: <code>android</code> , <code>iphone-ipad</code> , <code>mac</code> , or <code>windows-pc</code> . These are the device types that FortiClient currently supports. If the list is empty, all devices regardless of type are subject to FortiClient enforcement. The FortiClient enforcement portal must be enabled. | null |
| forticlient-compliance-enforcement-portal {enable disable} | Enable or disable the FortiClient enforcement portal. | disable |
| fsso {enable disable} | Enable or disable Fortinet Single Sign On. | disable |
| fsso-server-for-ntlm <server_str> | Restrict NTLM authentication to one particular server only for this policy. Enter the name of a server defined in user fsso . | No default. |
| geo-location {enable disable} | Enable or disable determining the country of each destination IP address. This is available when <code>auto-profiling</code> is enabled. | disable |
| global-label <label_str> | Put policy in the named subsection in the web-based manager. Subsection is created if it does not already exist. | No default. |
| gtp_profile <name_str> | For FortiOS Carrier, enter the name of a profile to add the GTP profile to the policy. | No default. |
| icap-profile <icap_pr_name> | Optionally, enter the name of an Internet Content Adaptation Protocol (ICAP) profile. This is available if <code>utm-status</code> is <code>enable</code> . | null |
| identity-based {enable disable} | Select to enable or disable identity-based policy authentication. This field appears only if <code>action</code> is <code>accept</code> . | disable |
| identity-based-route <idroute_name> | Optionally, specify an identity-based route to include. Identity-based routes are defined in firewall identity-based-route . | No default. |
| identity-from {auth device} | Select whether identity is based on authenticated user or device. This field is not available if <code>srcintf</code> is <code>web-proxy</code> . | auth |
| inbound {enable disable} | When <code>action</code> is set to <code>ipsec</code> , enable or disable traffic from computers on the remote private network to initiate an IPsec VPN tunnel. | disable |

| Variable | Description | Default |
|--|---|-------------|
| ip-based {enable disable} | If <code>srcintf</code> is <code>web-proxy</code> and <code>identity-based</code> is enabled, enable <code>ip-based</code> to handle FSSO authentication. Will cause an error if disabled when the firewall policy refers to directory based user groups such as FSSO. | disable |
| ippool {enable disable} | When the action is set to accept and NAT is enabled, configure a NAT policy to translate the source address to an address randomly selected from the first IP pool added to the destination interface of the policy. | disable |
| ips-sensor <name_str> | Enter the name of the IPS sensor to add to the firewall policy. This option appears only if <code>identity-based</code> is <code>disable</code> and <code>utm-status</code> is <code>enable</code> . | (null) |
| label <label_string> | Optionally, enter a label for this policy. The label is visible in the web-based manager in Section View. | No default. |
| logtraffic {all utm disable} | Choose which traffic logs will be recorded: <ul style="list-style-type: none"> all utm - only UTM-related logs disable - no logging | utm |
| logtraffic-app {enable disable} | Enable to log traffic while application logging is active. | enable |
| logtraffic-start {enable disable} | Enable to log session starts and ends. | disable |
| log-unmatched-traffic {disable enable} | Enable or disabling logging dropped traffic for policies with <code>identity-based</code> enabled. | disable |
| match-vip {enable disable} | If you want to explicitly drop a packet that is not matched with a firewall policy and write a log message when this happens, you can add a general policy (source and destination address set to ANY) to the bottom of a policy list and configure the firewall policy to DENY packets and record a log message when a packet is dropped. In some cases, when a virtual IP performs destination NAT (DNAT) on a packet, the translated packet may not be accepted by a firewall policy. If this happens, the packet is silently dropped and therefore not matched with the general policy at the bottom of the policy list. To catch these packets, enable <code>match-vip</code> in the general policy. Then the DNATed packets that are not matched by a VIP policy are matched with the general policy where they can be explicitly dropped and logged. | disable |
| mms-profile <name_str> | For FortiOS Carrier, enter the name of the MMS profile to add to the firewall policy. This option appears only if <code>identity-based</code> is <code>disable</code> and <code>utm-status</code> is <code>enable</code> . | (null) |

| Variable | Description | Default |
|---|---|--------------------|
| nat {enable disable} | Enable or disable network address translation (NAT). NAT translates the address and the port of packets accepted by the policy. When NAT is enabled, <code>ippool</code> and <code>fixedport</code> can also be enabled or disabled. This option appears only if <code>action</code> is <code>accept</code> or <code>ssl-vpn</code> . | disable |
| natinbound {enable disable} | Enable or disable translating the source addresses IP packets emerging from the tunnel into the IP address of the FortiGate unit's network interface to the local private network. This option appears only if <code>action</code> is <code>ipsec</code> . | disable |
| natip <address_ipv4mask> | When <code>action</code> is set to <code>ipsec</code> and <code>natoutbound</code> is enabled, specify the source IP address and subnet mask to apply to outbound clear text packets before they are sent through the tunnel. If you do not specify a <code>natip</code> value when <code>natoutbound</code> is enabled, the source addresses of outbound encrypted packets are translated into the IP address of the FortiGate unit's external interface. When a <code>natip</code> value is specified, the FortiGate unit uses a static subnetwork-to-subnetwork mapping scheme to translate the source addresses of outbound IP packets into corresponding IP addresses on the subnetwork that you specify. For example, if the source address in the firewall encryption policy is 192.168.1.0/24 and the <code>natip</code> value is 172.16.2.0/24, a source address of 192.168.1.7 will be translated to 172.16.2.7. | 0.0.0.0 0.0.0.0 |
| natoutbound {enable disable} | When <code>action</code> is set to <code>ipsec</code> , enable or disable translating the source addresses of outbound encrypted packets into the IP address of the FortiGate unit's outbound interface. Enable this attribute in combination with the <code>natip</code> attribute to change the source addresses of IP packets before they go into the tunnel. | disable |
| netscan-discover-hosts {enable disable} | Enable host discovery for hostname visibility feature. Available when <code>utm-status</code> is enabled. | disable |
| ntlm {enable disable} | Enable or disable Directory Service authentication via NTLM. If you enable this option, you must also define the user groups. This option appears only if <code>identity-based</code> is <code>enable</code> . | disable |
| ntlm-enabled-browsers <user-agent_string> | Enter the HTTP-User-Agent strings of supported browsers. Enclose each string in quotes and separate strings with a space. Browsers with non-matching strings get guest access. | No default. |
| ntlm-guest {enable disable} | Enable or disable NTLM guest user access. | disable |

| Variable | Description | Default |
|--|--|-------------|
| outbound {enable disable} | When <code>action</code> is set to <code>ipsec</code> , enable or disable traffic from computers on the local private network to initiate an IPSec VPN tunnel. | disable |
| per-ip-shaper <shaper_name> | Enter the name of the per-IP traffic shaper to apply. For information about per-IP traffic shapers, see firewall shaper per-ip-shaper . | No default. |
| permit-any-host {enable disable} | Enable to accept UDP packets from any host. This can help support the FaceTime application on NAT'd iPhones. | disable |
| permit-stun-host {enable disable} | Enable to accept UDP packets from any STUN host. This can help support the FaceTime application on NAT'd iPhones. | disable |
| poolname <name_str> | Enter the name of the IP pool. This variable appears only if <code>nat</code> and <code>ippool</code> are enable. | No default. |
| profile-type {group single} | Select whether to add individual UTM profiles or a UTM profile group to the firewall policy. This option is available in this context level only if the <code>identity-based</code> option is set to <code>disable</code> . If <code>identity-based</code> is set to <code>enable</code> this option will instead be available in each Authentication Rule in the config identity-based-policy sub section. | single |
| profile-group <name_str> | Enter the name of a UTM profile group to add to the firewall policy. This option is available if <code>profile-type</code> is set to <code>group</code> . This option is available in this context level only if, at this context level the <code>identity-based</code> option is set to <code>disable</code> and <code>utm-status</code> is set to <code>enable</code> . If <code>identity-based</code> is set to <code>enable</code> this option may be available within Authentication rules in the config identity-based-policy sub section. | (null) |
| profile-protocol-options <name_str> | Enter the name of the protocol options profile to add to the firewall policy. This option is available in this context level only if, at this context level the <code>identity-based</code> option is set to <code>disable</code> and <code>utm-status</code> is set to <code>enable</code> . If <code>identity-based</code> is set to <code>enable</code> this option may be available within Authentication rules in the config identity-based-policy sub section. | (null) |
| redirect-url <name_str> | Enter a URL, if any, that the user is redirected to after authenticating and/or accepting the user authentication disclaimer. This option only appears if <code>disclaimer</code> is enable. | No default. |
| replacemsg-group <name_str> | For FortiOS Carrier, enter the name of the replacement message group to add to the firewall policy. This option appears only if <code>identity-based</code> is <code>disable</code> and <code>utm-status</code> is <code>enable</code> . | default |

| Variable | Description | Default |
|---|--|-------------|
| replacemsg-override-group <group_string> | Select a replacement message override group from the available configured groups. This will override the default replacement message for this policy. | |
| require-tfa {enable disable} | Enable to require two-factor authentication. | disable |
| rsso {enable disable} | Enable or disable RADIUS-based single sign-on (SSO) for this policy. | disable |
| rtp-nat {disable enable} | Enable to apply source NAT to RTP packets received by the firewall policy. This field is used for redundant SIP configurations. If <code>rtp-nat</code> is enabled you must add one or more firewall addresses to the <code>rtp-addr</code> field. | disable |
| rtp-addr <name_str> | Enter one or more RTP firewall addresses for the policy. Separate multiple firewall addresses with a space. This field is only available when <code>rtp-nat</code> is enabled. | |
| schedule <name_str> | Enter the name of the one-time or recurring schedule or schedule group to use for the policy. | No default. |
| schedule-timeout {enable disable} | Enable to force session to end when policy schedule end time is reached. | disable |
| send-deny-packet {enable disable} | Enable to send a packet in reply to denied TCP, UDP or ICMP traffic. When <code>deny-tcp-with-icmp</code> is enabled in system settings , a Communication Prohibited ICMP packet is sent. Otherwise, denied TCP traffic is sent a TCP reset. | disable |
| service <name_str> | Enter the name of one or more services, or a service group, to match with the firewall policy. Separate multiple services with a space. | No default. |
| service-negate {enable disable} | Enable to negate <code>service</code> match. This causes <code>service</code> to specify what the service must not be. | disable |
| sessions {enable disable} | Enable or disable taking a snapshot of the number of active sessions for the policy every five minutes. This is available when <code>auto-profiling</code> is enabled. | disable |
| session-ttl <session_time_int> | Set the timeout value in the policy to override the global timeout setting defined by using <code>config system session-ttl</code> . When it is on default value, it will not take effect. | 0 |
| spamfilter-profile <name_str> | Enter the name of the email filter profile to add to the firewall policy. This option appears only if <code>identity-based</code> is <code>disable</code> and <code>utm-status</code> is <code>enable</code> . To add a <code>spamfilter-profile</code> , you must obtain an adequate profile name in <code>profile-protection-options</code> . | (null) |

| Variable | Description | Default |
|--|--|-------------|
| srcaddr <name_str> srcaddr6 <name_str> | <p>Enter one or more source firewall addresses for the policy. Separate multiple firewall addresses with a space.</p> <p>Use <code>srcaddr6</code> for IPv6 addresses.</p> <p>If <code>action</code> is set to <code>ipsec</code>, enter the private IP address of the host, server, or network behind the FortiGate unit.</p> <p>If <code>action</code> is set to <code>ssl-vpn</code> and the firewall encryption policy is for web-only mode clients, type <code>all</code>.</p> <p>If <code>action</code> is set to <code>ssl-vpn</code> and the firewall encryption policy is for tunnel mode clients, enter the name of the IP address range that you reserved for tunnel mode clients. To define an address range for tunnel mode clients, see “ssl settings” on page 816.</p> | No default. |
| srcaddr-negate {enable disable} | <p>Enable to negate <code>srcaddr</code> match. This causes <code>srcaddr</code> to specify what the source address must not be.</p> | disable |
| srcintf <name_str> | <p>Enter the source interface(s) for the policy. Separate interface names with spaces.</p> <p>The interface can be a physical interface, a VLAN subinterface, a zone, ftp-proxy, or web-proxy.</p> <p>If the interface or VLAN subinterface has been added to a zone, interface or VLAN subinterface cannot be used for <code>srcintf</code>.</p> <p>If <code>action</code> is set to <code>ipsec</code>, enter the name of the interface to the local (private) network.</p> <p>If <code>action</code> is set to <code>ssl-vpn</code>, enter the name of the interface that accepts connections from remote clients.</p> | No default. |
| sslvpn-auth {any ldap local radius tacacs+} | <p>If <code>action</code> is set to <code>ssl-vpn</code>, enter one of the following client authentication options:</p> <ul style="list-style-type: none"> If you want the FortiGate unit to authenticate remote clients using any local user group, a RADIUS server, or LDAP server, type <code>any</code>. If the user group is a local user group, type <code>local</code>. If the remote clients are authenticated by an external RADIUS server, type <code>radius</code>. If the remote clients are authenticated by an external LDAP server, type <code>ldap</code>. If the remote clients are authenticated by an external TACACS+ server, type <code>tacacs+</code>. <p>You must also set the name of the group which will use the authentication method.</p> | any |
| sslvpn-ccert {enable disable} | <p>If <code>action</code> is set to <code>ssl-vpn</code>, enable or disable the use of security certificates to authenticate remote clients. If <code>sslvpn-ccert</code> is enabled, the SSLVPN daemon will require a client certificate for the users defined in the policy.</p> | disable |

| Variable | Description | Default |
|-------------------------------------|---|-------------|
| sslvpn-cipher {any medium high} | If <code>action</code> is set to <code>ssl-vpn</code> , enter one of the following options to determine the level of SSL encryption to use. <ul style="list-style-type: none"> high is 164-bit or greater cipher suite. medium is 128-bit or greater cipher suite. | any |
| sso-auth-method {fssso rssso} | Select the passive authentication method to use with FSSO/RSSO. If it fails, <code>active-auth-method</code> is used, if set. | null |
| status {enable disable} | Enable or disable the policy. | enable |
| tags <tags_str> | Enter object tags applied to this policy. Separate tag names with spaces. | null |
| tcp-mss-sender <maximumsize_int> | Enter a TCP Maximum Sending Size number for the sender. When a FortiGate unit is configured to use PPPoE to connect to an ISP, certain web sites may not be accessible to users. This occurs because a PPPoE frame takes an extra 8 bytes off the standard Ethernet MTU of 1500. When the server sends the large packet with DF bit set to 1, the ADSL provider's router either does not send an "ICMP fragmentation needed" packet or the packet is dropped along the path to the web server. In either case, the web server never knows fragmentation is required to reach the client. In this case, configure the <code>tcp-mss-sender</code> option to enable access to all web sites. For more information, see the article Cannot view some web sites when using PPPoE on the Fortinet Knowledge Center. | 0 |
| tcp-mss-receiver <maximumsize_int> | Enter a TCP MSS number for the receiver. | 0 |
| timeout-send-rst {enable disable} | Enable sending a TCP reset when an application session times out. | disable |
| traffic-shaper <name_str> | Select a traffic shaper for the policy. A traffic shaper controls the bandwidth available to, and sets the priority of the traffic processed by, the policy. This option appears only if <code>identity-based</code> is <code>disable</code> . | No default. |
| traffic-shaper-reverse <name_str> | Select a reverse traffic shaper. For example, if the traffic direction that a policy controls is from port1 to port2, select this option will also apply the policy shaping configuration to traffic from port2 to port1. | No default. |
| utm-status {disable enable} | Enable or disable UTM for the firewall policy. If you enable UTM you must add one or more UTM profiles and sensors (or a group profile) to the firewall policy. This option is available in this context level only if the <code>identity-based</code> option is set to <code>disable</code> . If <code>identity-based</code> is set to <code>enable</code> this option will instead be available in each Authentication Rule in the config identity-based-policy sub section. | disable |

| Variable | Description | Default |
|---|--|-------------|
| voip-profile <name_str> | Enter the name of the VoIP profile to add to the firewall policy. This option appears only if <code>identity-based</code> is <code>disable</code> and <code>utm-status</code> is <code>enable</code> . | (null) |
| vpntunnel <name_str> | Enter the name of a Phase 1 IPsec VPN configuration to apply to the tunnel. This option appears only if <code>action</code> is <code>ipsec</code> . | No default. |
| wanopt {enable disable} | Enable or disable WAN optimization on this policy. WANOpt is available only if <code>action</code> is <code>accept</code> . | disable |
| wanopt-detection {active passive off} | Select WANOpt peer auto-detection mode. | off |
| wanopt-profile <name_str> | Enter the WANOpt profile to use in this policy. | No default. |
| wanopt-peer <peer_name> | Enter the WAN Optimization peer. | No default. |
| wccp {enable disable} | Enable or disable web cache on the policy. If enabled, the FortiGate unit will check the learned web cache information, and may redirect the traffic to the web cache server. | disable |
| web-auth-cookie {enable disable} | Enable to reduce the number of authentication requests to the authentication server when session-based authentication is applied using explicit web proxy. This is only available when session based authentication is enabled. | disable |
| webcache {disable enable} | Enable or disable WAN optimization web caching for HTTP traffic accepted by the firewall policy. This option is available only on FortiGate units that support WAN Optimization and web caching. | disable |
| webcache-https {disable any ssl-server} | Enable the level of webcaching for HTTPS traffic. <code>disable</code> — no caching of HTTPS traffic <code>any</code> — use SSL offload for traffic of matched SSL server. For other HTTPS traffic, it intercepts in the same way as HTTPS deep scan. <code>ssl-server</code> — cache only traffic of matched SSL server whose port matches the HTTPS port in the protocol option or 443 if protocol option is not defined. This field is not available if <code>srcintf</code> is <code>ftp-proxy</code> or <code>wanopt</code> . | disable |
| webfilter-profile <name_str> | Enter the name of the web filtering profile to add to the firewall policy. This option appears only if <code>identity-based</code> is <code>disable</code> and <code>utm-status</code> is <code>enable</code> . To add a <code>webfilter-profile</code> , you must obtain an adequate profile name in <code>profile-protection-options</code> . | (null) |

| Variable | Description | Default |
|--|--|-------------|
| webproxy-forward-server <fwd_srv_name_string> | Enter the name of the web-proxy forward server. Available if <code>srcintf</code> is <code>web-proxy</code> . | No default. |
| wsso {enable disable} | Enable or disable WiFi Single Sign On. | disable |

config identity-based-policy

Create an identity-based firewall policy that requires authentication. This option is only available if `identity-based` is enabled.

| Variable | Description | Default |
|---|--|-----------------------|
| <policy_id> | Enter the name for the identity-based policy. | No default. |
| action {accept deny capture} | Select the action for this policy: accept, deny, or route to captive portal. | accept |
| application-list <name_str> | Enter the name of the application list to add to the identify-based policy. | (null) |
| av-profile <name_str> | Enter the name of the antivirus profile to add to the identify-based policy. | (null) |
| captive-portal {device-identification email-collection forticlient-download} | Select the type of captive portal. Available when <code>action</code> is <code>capture</code> . | device-identification |
| client-reputation {enable disable} | Enable or disable client reputation feature on this policy. <code>utm-status</code> must be enabled. | disable |
| deep-inspection-options <profile_name> | Enter the name of the deep inspection options profile to apply. See “firewall deep-inspection-options” on page 109 . | No default. |
| devices <device_list> | Enter the device categories to which this policy applies. | No default. |
| dlp-sensor <name_str> | Enter the name of the DLP sensor to add to the identify-based policy. To add a <code>dlp-sensor</code> , you must obtain an adequate name in <code>profile-protection-options</code> . | (null) |
| endpoint-compliance {enable disable} | Enable or disable Endpoint control. | disable |
| groups <group_name> | Enter the user group name for the identity-based policy. | No default. |
| ips-sensor <name_str> | Enter the name of the IPS sensor to add to the identify-based policy. | (null) |
| logtraffic {enable disable} | Enable or disable traffic logging for the identity-based policy. | disable |
| mms-profile <name_str> | For FortiOS Carrier, enter the name of the MMS profile to add to the identify-based policy. | (null) |
| per-ip-shaper <name_str> | Enter the per-IP traffic shaper for the identity-based policy. | No default. |
| profile-group {group single} | Enter the name of a UTM profile group to add to the identity-based policy. This option is available if <code>profile-type</code> is set to <code>group</code> . | (null) |
| profile-protocol-options <name_str> | Enter the name of the protocol options profile to add to the firewall policy. | (null) |

| Variable | Description | Default |
|-----------------------------------|--|-------------|
| profile-type {group single} | Select whether to add individual UTM profiles or a UTM profile group to the identity-based policy. | single |
| schedule <name_str> | Enter the firewall schedule for the identity-based policy. | No default. |
| service <name_str> | Enter the firewall service for the identity-based policy. | No default. |
| spamfilter-profile <name_str> | Enter the name of the email filter profile to add to the identify-based policy. | (null) |
| sslvpn-realm <realm-url-path> | Optionally, enter the SSL VPN realm URL (without “http://”). This is available when action is ssl-vpn. | No default. |
| traffic-shaper <name_str> | Enter the traffic shaper for the identity-based policy. | No default. |
| traffic-shaper-reverse <name_str> | Enter the reverse direction traffic shaper for the identity-based policy. | No default. |
| users <user_name_list> | Enter the users to whom this policy applies. Separate names with spaces. | No default. |
| utm-status {disable enable} | Enable or disable UTM for the identity-based policy. If you enable UTM you must add one ore more UTM profiles and sensors (or a profile group) to the identify-based policy. | disable |
| voip-profile <name_str> | Enter the name of the VoIP profile to add to the identify-based policy. | (null) |
| webfilter-profile <name_str> | Enter the name of the web filtering profile to add to the identify-based policy. | (null) |

policy46, policy64

Use this command to configure IPv6 <-> IPv4 policies.

- Use `config firewall policy46` for IPv4-to-IPv6 policies
- Use `config firewall policy64` for IPv6-to-IPv4 policies

Syntax

```
config firewall policy46 or config firewall policy64
edit <index_int>
    set action {accept | deny}
    set comments <comment_str>
    set dstaddr <name_str>
    set dstintf <name_str>
    set fixedport {enable | disable}
    set ippool {enable | disable}
    set logtraffic {enable | disable}
    set per-ip-shaper <shaper_name>
    set poolname <name_str>
    set schedule <name_str>
    set service <name_str>
    set srcaddr <name_str>
    set srcintf <name_str>
    set status {enable | disable}
    set tags <tags_str>
    set traffic-shaper <name_str>
    set traffic-shaper-reverse <name_str>
end
```

| Variable | Description | Default |
|---------------------------|---|-------------|
| <index_int> | Enter the unique ID number of this policy. | No default. |
| action {accept deny} | <p>Select the action that the FortiGate unit will perform on traffic matching this firewall policy.</p> <ul style="list-style-type: none"> • accept: Allow packets that match the firewall policy. Also enable or disable <code>ippool</code> to select a source address for packets from a pool of IP addresses added to the destination interface and enable or disable <code>fixedport</code> so that the policy does not translate the packet source port. • deny: Deny packets that match the firewall policy. | deny |
| comments <comment_str> | <p>Enter a description or other information about the policy. (Optional)</p> <p><code>comment_str</code> is limited to 63 characters. Enclose the string in single quotes to enter special characters or spaces.</p> | No default. |
| dstaddr <name_str> | Enter one or more destination firewall addresses. Separate multiple firewall addresses with a space. | No default. |

| Variable | Description | Default |
|--------------------------------------|--|-------------|
| dstintf <name_str> | Enter the destination interface for the policy. The interface can be a physical interface, a VLAN subinterface, or a zone. Note: If a interface or VLAN subinterface has been added to a zone, the interface or VLAN subinterface cannot be used for dstintf. | No default. |
| fixedport {enable disable} | Enable to preserve packets' source port number. Some applications do not function correctly if the source port number is changed, and may require this option. If fixedport is enable, you should usually also enable IP pools; if you do not configure an IP pool for the policy, only one connection can occur at a time for this port. | disable |
| ippool {enable disable} | Enable translating the source address to an address randomly selected from the first IP pool added to the destination interface of the policy. | disable |
| logtraffic {enable disable} | Enable or disable recording traffic log messages for this policy. | disable |
| per-ip-shaper <shaper_name> | Enter the name of the per-IP traffic shaper to apply. For information about per-IP traffic shapers, see firewall shaper per-ip-shaper . | No default. |
| poolname <name_str> | Enter the name of the IP pool. This variable appears only if ippool is enable. | No default. |
| schedule <name_str> | Enter the name of the one-time or recurring schedule or schedule group to use for the policy. | No default. |
| service <name_str> | Enter the name of one or more services, or a service group, to match with the firewall policy. Separate multiple services with a space. | No default. |
| srcaddr <name_str> | Enter one or more source firewall addresses for the policy. Separate multiple firewall addresses with a space. | No default. |
| srcintf <name_str> | Enter the source interface for the policy. If the interface or VLAN subinterface has been added to a zone, interface or VLAN subinterface cannot be used for srcintf. | No default. |
| status {enable disable} | Enable or disable the policy. | enable |
| tags <tags_str> | Enter object tags applied to this policy. Separate tag names with spaces. | null |
| traffic-shaper <name_str> | Select a traffic shaper for the policy. A traffic shaper controls the bandwidth available to, and sets the priority of the traffic processed by, the policy. | No default. |
| traffic-shaper-reverse <name_str> | Select a reverse traffic shaper. For example, if the traffic direction that a policy controls is from port1 to port2, select this option will also apply the policy shaping configuration to traffic from port2 to port1. | No default. |

profile-group

Use this command in FortiOS Carrier to create profile groups. A profile group can contain an antivirus profile, IPS sensor, web filter profile, email filter profile, DLP sensor, application control list, a VoIP profile, an MMS profile and a replacement message group. Once you create profile groups you can add them to firewall policies instead of adding individual UTM profiles and lists.

Syntax

```
config firewall profile-group
edit <name_str>
    set profile-protocol-options <name_str>
    set deep-inspection-options <profile_name>
    set av-profile <name_str>
    set icap-profile <name_str>
    set webfilter-profile <name_str>
    set spamfilter-profile <name_str>
    set ips-sensor <name_str>
    set dlp-sensor <name_str>
    set application-chart {top10-app | top10-media-user | top10-p2p-user}
    set application-list <name_str>
    set voip-profile <name_str>
    set mms-profile <name_str>
    set replacemsg-group <name_str>
end
```

| Variable | Description | Default |
|--|--|-------------|
| <name_str> | Enter the name of the profile group. | |
| profile-protocol-options <name_str> | Enter the name of the protocol options profile to add to the profile group. | (null) |
| deep-inspection-options <profile_name> | Enter the name of the deep inspection options profile to apply. See “firewall deep-inspection-options” on page 109 . | No default. |
| av-profile <name_str> | Enter the name of the antivirus profile to add to the profile group. To add an av-profile, you must obtain an adequate profile name in profile-protection-options. | (null) |
| icap-profile <name_str> | Enter the name of the Internet Content Adaptation Protocol (ICAP) profile to add to the profile group. To add an icap-profile, you must obtain an adequate profile name in profile-protection-options. | (null) |
| webfilter-profile <name_str> | Enter the name of the web filtering profile to add to the profile group. To add a webfilter-profile, you must obtain an adequate profile name in profile-protection-options. | (null) |
| spamfilter-profile <name_str> | Enter the name of the email filter profile to add to the profile group. To add a spamfilter-profile, you must obtain an adequate profile name in profile-protection-options. | (null) |
| ips-sensor <name_str> | Enter the name of the IPS sensor to add to the profile group. | (null) |

| Variable | Description | Default |
|--|--|---------|
| dlp-sensor <name_str> | Enter the name of the DLP sensor to add to the profile group. To add an dlp-sensor, you must obtain an adequate profile name in profile-protection-options. | (null) |
| application-chart {top10-app top10-media-user top10-p2p-user} | Enter the application chart type. <ul style="list-style-type: none"> • top10-app: Top 10 applications chart • top10-media-user: Top 10 media users chart • top10-p2p-user: Top 10 P2P users chart | (null) |
| application-list <name_str> | Enter the name of the application list to add to the profile group. | (null) |
| voip-profile <name_str> | Enter the name of the VoIP profile to add to the profile group. | (null) |
| mms-profile <name_str> | For FortiOS Carrier, enter the name of the MMS profile to add to the profile group. | (null) |
| replacemsg-group <name_str> | For FortiOS Carrier, enter the name of the replacement message group to add to the profile group. | default |

profile-protocol-options

Use this command to configure UTM protocol options profiles for firewall policies. Protocol options configure how UTM functionality identifies content protocols such as HTTP, FTP, and SMTP. Every firewall policy that includes UTM profiles must include a protocol options profile.

SSL-related options for secure protocols are set in [firewall deep-inspection-options](#).

Syntax

```
config firewall profile-protocol-options
  edit <name_str>
    set comment <comment_str>
    set oversize-log {disable | enable}
    set intercept-log {enable | disable}
    config http
      set ports <port_number_list>
      set inspect-all {enable | disable}
      set options {chunkedbypass | clientcomfort
        | no-content-summary | oversize | servercomfort}
      set comfort-interval <interval_int>
      set comfort-amount <amount_int>
      set post-lang <charset1> [<charset2>... <charset5>]
      set oversize-limit <size_int>
      set retry-count <retry_int>
    end
    config ftp
      set ports <port_number_list>
      set inspect-all {disable | enable}
      set options {bypass-mode-command | bypass-rest-command
        | clientcomfort | no-content-summary | oversize
        | splice}
      set comfort-interval <interval_int>
      set comfort-amount <amount_int>
      set post-lang <charset1> [<charset2>... <charset5>]
      set oversize-limit <size_int>
      set status {enable | disable}
    end
    config dns
      set ports <dns_port_list>
      set status {enable | disable}
    end
    config imap
      set ports <port_number_list>
      set inspect-all {enable | disable}
      set options {fragmail | no-content-summary | oversize}
      set oversize-limit <size_int>
      set status {enable | disable}
    end
  end
```

```

config mapi
    set ports <port_number_list>
    set options {fragmail | no-content-summary | oversize}
    set oversize-limit <size_int>
    set status {enable | disable}
end
config pop3
    set ports <port_number_list>
    set inspect-all {enable | disable}
    set options {fragmail | no-content-summary | oversize}
    set oversize-limit <size_int>
    set status {enable | disable}
end
config smtp
    set ports <port_number_list>
    set inspect-all {enable | disable}
    set options {fragmail | no-content-summary | oversize
                | splice}
    set oversize-limit <size_int>
    set server_busy {enable | disable}
    set status {enable | disable}
end
config nntp
    set ports <port_number_list>
    set inspect-all {disable | enable}
    set options { no-content-summary | oversize | splice}
    set oversize-limit <size_int>
    set status {enable | disable}
end
config im
    set options { no-content-summary | oversize}
    set oversize-limit <size_int>
    set status {enable | disable}
end
config mail-signature
    set status {enable | disable}
    set signature <text>
end
end

```

| Variable | Description | Default |
|----------------------------------|--|---------|
| <name_str> | Enter the name of the protocol options profile. | |
| comment <comment_str> | Optionally enter a description of up to 63 characters of the protocol options profile. | |
| oversize-log {disable enable} | Enable or disable logging for antivirus oversize file blocking. | disable |
| intercept-log {enable disable} | Enable or disable logging for FortiOS Carrier antivirus file filter is set to intercept. | |

config http

Configure HTTP protocol options.

| Variable | Description | Default |
|---|--|--------------------|
| ports <port_number_list> | Enter a space-separated list of port numbers to scan for HTTP content. | 80 |
| inspect-all {enable disable} | Enable to monitor all ports for the HTTP protocol. If you enable this option you can't select a port. | disable |
| options {chunkedbypass clientcomfort no-content-summary oversize servercomfort} | <p>Select one or more options apply to HTTP sessions. To select more than one, enter the option names separated by a space.</p> <p>chunkedbypass — allow web sites that use chunked encoding for HTTP to bypass the firewall. Chunked encoding means the HTTP message body is altered to allow it to be transferred in a series of chunks. Use of this feature is a risk. Malicious content could enter the network if web content is allowed to bypass the firewall.</p> <p>clientcomfort — apply client comforting and prevent client timeout.</p> <p>no-content-summary — do not add content information from the dashboard.</p> <p>oversize — block files that are over the file size limit.</p> <p>servercomfort — apply server comforting and prevent server timeout.</p> | no-content-summary |
| comfort-interval <interval_int> | Enter the time in seconds to wait before client comforting starts after a download has begun. It is also the interval between subsequent client comforting sends. The range is 1 to 900 seconds. | 10 |
| comfort-amount <amount_int> | Enter the number of bytes client comforting sends each interval to show that an HTTP download is progressing. The range is 1 to 10240 bytes. | 1 |
| fortinet-bar {enable disable} | Enable or disable Fortinet Bar on HTML pages. | |
| fortinet-bar-port <port_int> | Specify port for Fortinet Bar. | 8011 |
| post-lang <charset1> [<charset2>... <charset5>] | <p>For HTTPS post pages, because character sets are not always accurately indicated in HTTPS posts, you can use this option to specify up to five character set encodings. The FortiGate unit performs a forced conversion of HTTPS post pages to UTF-8 for each specified character set. After each conversion the FortiGate unit applies web content filtering and DLP scanning to the content of the converted page.</p> <p>Specifying multiple character sets reduces web filtering and DLP performance.</p> | |

| Variable | Description | Default |
|--------------------------------------|--|---------|
| oversize-limit <size_int> | Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the <code>oversize-limit</code> , the file is passed or blocked, depending on whether <code>oversize</code> is a selected HTTP option. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM. | 10 |
| retry-count <retry_int> | Enter the number of times to retry establishing an HTTP connection when the connection fails on the first try. The range is 0 to 100. This allows the web server proxy to repeat the connection attempt on behalf of the browser if the server refuses the connection the first time. This works well and reduces the number of hang-ups or page not found errors for busy web servers. Entering zero (0) effectively disables this feature. | 0 |
| status {enable disable} | Enable or disable HTTP protocol inspection. | enable |
| switching-protocols {block bypass} | Choose whether when the protocol switches, the new protocol is blocked or bypassed from scanning. | bypass |

config ftp

Configure FTP protocol options.

| Variable | Description | Default |
|---------------------------------|--|---------|
| ports <port_number_list> | Enter a space-separated list of port numbers to scan for FTP content. | 21 |
| inspect-all {disable enable} | Enable to monitor all ports for the FTP protocol. If you enable this option you can't select a port. | disable |
| comfort-interval <interval_int> | Enter the time in seconds to wait before client comforting starts after a download has begun. It is also the interval between subsequent client comforting sends. The range is 1 to 900 seconds. | 10 |
| comfort-amount <amount_int> | Enter the number of bytes client comforting sends each interval to show that an FTP download is progressing. The range is 1 to 10240 bytes. | 1 |

| Variable | Description | Default |
|---|--|------------------------------|
| options {bypass-mode-command bypass-rest-command clientcomfort no-content-summary oversize splice} | <p>Select one or more options apply to FTP sessions. To select more than one, enter the option names separated by a space.</p> <p><code>bypass-mode-command</code> — if the MODE command is issued with 'block' or 'compressed', disable content scanning until the setting changes or a new command is issued.</p> <p><code>bypass-rest-command</code> — if the REST command is issued with a value other than 0, disable content scanning until the setting changes or a new command is issued.</p> <p><code>clientcomfort</code> — apply client comforting and prevent client timeout.</p> <p><code>no-content-summary</code> — do not add content information from the dashboard.</p> <p><code>oversize</code> — block files that are over the file size limit.</p> <p><code>splice</code> — simultaneously scan a file and send it to the recipient. If the FortiGate unit detects a virus, it prematurely terminates the connection.</p> | no-content-summary splice |
| oversize-limit <size_int> | Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the <code>oversize-limit</code> , the file is passed or blocked depending on whether <code>oversize</code> is a selected FTP option. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM. | 10 |
| status {enable disable} | Enable or disable FTP protocol inspection. | enable |

config dns

Configure DNS protocol options.

| Variable | Description | Default |
|---------------------------|---|---------|
| ports <dns_port_list> | Enter a space-separated list of port numbers to scan for DNS content. | 53 |
| status {enable disable} | Enable or disable DNS protocol inspection. | enable |

config imap

Configure IMAP protocol options.

| Variable | Description | Default |
|-----------------------------------|---|---------|
| ports <port_number_list> | Enter a space-separated list of port numbers to scan for IMAP content. | 143 |
| inspect-all {enable disable} | Enable to monitor all ports for the IMAP protocol. If you enable this option you can't select a port. | disable |

| Variable | Description | Default |
|--|--|--------------------------------|
| options { fragmail no-content-summary oversize } | Select one or more options apply to IMAP sessions. To select more than one, enter the option names separated by a space. fragmail — allow fragmented email. Fragmented email cannot be scanned for viruses. no-content-summary — do not add content information from the dashboard. oversize — block files that are over the file size limit. | fragmail no-content-summary |
| oversize-limit <size_int> | Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the oversize-limit, the file is passed or blocked depending on whether oversize is a selected IMAP option. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM. | 10 |
| status { enable disable } | Enable or disable IMAP protocol inspection. | enable |

config mapi

Configure MAPI protocol options.

| Variable | Description | Default |
|--|--|--------------------------------|
| ports <port_number_list> | Enter a space-separated list of port numbers to scan for MAPI content. | 135 |
| options { fragmail no-content-summary oversize } | Select one or more options apply to MAPI sessions. To select more than one, enter the option names separated by a space. fragmail — allow fragmented email. Fragmented email cannot be scanned for viruses. no-content-summary — do not add content information from the dashboard. oversize — block files that are over the file size limit. | fragmail no-content-summary |
| oversize-limit <size_int> | Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the oversize-limit, the file is passed or blocked depending on whether oversize is a selected MAPI option. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM. | 10 |
| status { enable disable } | Enable or disable MAPI protocol inspection. | enable |

config pop3

Configure POP3 protocol options.

| Variable | Description | Default |
|-------------------------------------|---|---------|
| ports <port_number_list> | Enter a space-separated list of port numbers to scan for POP3 content. | 110 |
| inspect-all { enable disable } | Enable to monitor all ports for the POP3 protocol. If you enable this option you can't select a port. | disable |

| Variable | Description | Default |
|--|--|--|
| options { fragmail no-content-summary oversize } | Select one or more options apply to POP3 sessions. To select more than one, enter the option names separated by a space. fragmail — allow fragmented email. Fragmented email cannot be scanned for viruses. no-content-summary — do not add content information from the dashboard. oversize — block files that are over the file size limit. | fragmail no- content- summary |
| oversize-limit <size_int> | Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the oversize-limit, the file is passed or blocked depending on whether oversize is a selected POP3 option. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM. | 10 |
| status { enable disable } | Enable or disable POP3 protocol inspection. | enable |

config smtp

Configure SMTP protocol options.

| Variable | Description | Default |
|---|--|--|
| ports <port_number_list> | Enter a space-separated list of port numbers to scan for SMTP content. | 25 |
| inspect-all { enable disable } | Enable to monitor all ports for the SMTP protocol. If you enable this option you can't select a port. | disable |
| options { fragmail no-content-summary oversize splice } | Select one or more options apply to SMTP sessions. To select more than one, enter the option names separated by a space. fragmail allow fragmented email. Fragmented email cannot be scanned for viruses. no-content-summary — do not add content information from the dashboard. oversize — block files that are over the file size limit. splice — simultaneously scan a message and send it to the recipient. If the FortiGate unit detects a virus, it prematurely terminates the connection, and returns an error message to the sender, listing the virus and infected file name. splice is selected when scan is selected. With streaming mode enabled, select either Spam Action (Tagged or Discard) for SMTP spam. When streaming mode is disabled for SMTP, infected attachments are removed and the email is forwarded (without the attachment) to the SMTP server for delivery to the recipient. Throughput is higher when streaming mode is enabled. | fragmail no- content- summary splice |

| Variable | Description | Default |
|-----------------------------------|---|---------|
| oversize-limit <size_int> | Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the <code>oversize-limit</code> , the file is passed or blocked depending on whether <code>oversize</code> is a selected SMTP option. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM. | 10 |
| server_busy {enable disable} | <p>Enable this options so that when the FortiGate unit attempts to send an SMTP email but can't because of a connection timeout or connection error it returns a 412 server busy error message to the email client attempting to send the message.</p> <p>Usually the FortiGate unit accepts SMTP SYN from clients and immediately send back ACK before actually connecting with the real SMTP server. If the server responds back with NACK (service not available) the FortiGate-to-server connection drops, but the FortiGate-to-client connection will just hang until a timeout occurs. This causes particular problems for systems that use alternative servers, they may not move to the next server until the timeout occurs. Not all SMTP mail servers behave in this way, some use an SMTP HELO to confirm the connection is active and so do not have an issue with this behavior.</p> | disable |
| status {enable disable} | Enable or disable SMTP protocol inspection. | enable |

config nntp

Configure NNTP protocol options.

| Variable | Description | Default |
|---|--|--------------------|
| ports <port_number_list> | Enter a space-separated list of port numbers to scan for NNTP content. | 119 |
| inspect-all {disable enable} | Enable to monitor all ports for the NNTP protocol. If you enable this option you can't select a port. | disable |
| options { no-content-summary oversize splice} | <p>Select one or more options apply to NNTP sessions. To select more than one, enter the option names separated by a space.</p> <p><code>no-content-summary</code> — do not add content information from the dashboard.</p> <p><code>oversize</code> — block files that are over the file size limit.</p> <p><code>splice</code> — simultaneously scan a file and send it to the recipient. If the FortiGate unit detects a virus, it prematurely terminates the connection.</p> | no-content-summary |

| Variable | Description | Default |
|------------------------------|---|---------|
| oversize-limit <size_int> | Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the <code>oversize-limit</code> , the file is passed or blocked depending on whether <code>oversize</code> is a selected NNTP option. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM. | 10 |
| status {enable disable} | Enable or disable NNTP protocol inspection. | enable |

config im

Configure IM protocol options.

| Variable | Description | Default |
|--|---|--------------------|
| options { no-content-summary oversize} | Select one or more options apply to IM sessions. To select more than one, enter the option names separated by a space. <code>no-content-summary</code> — do not add content information from the dashboard. <code>oversize</code> — block files that are over the file size limit. | no-content-summary |
| oversize-limit <size_int> | Enter the maximum in-memory file size that will be scanned, in megabytes. If the file is larger than the <code>oversize-limit</code> , the file is passed or blocked depending on whether <code>oversize</code> is a selected IM option. The maximum file size for scanning in memory is 10% of the FortiGate unit's RAM. | 10 |
| status {enable disable} | Enable or disable IM protocol inspection. | enable |

config mail-signature

Configure email signature options for SMTP.

| Variable | Description | Default |
|------------------------------|--|---------|
| status {enable disable} | Enable or disable adding an email signature to SMTP email messages as they pass through the FortiGate unit. | disable |
| signature <text> | Enter a signature to add to outgoing email. If the signature contains spaces, surround it with single or double quotes (' or "). | (null) |

schedule onetime

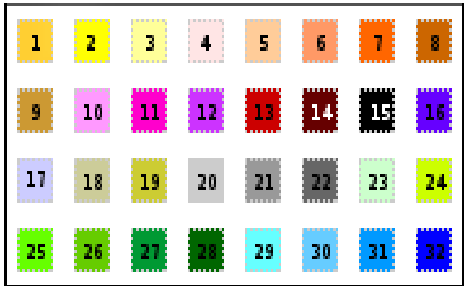
Use this command to add, edit, or delete one-time schedules.

Use scheduling to control when policies are active or inactive. Use one-time schedules for policies that are effective once for the period of time specified in the schedule.

To edit a schedule, define the entire schedule, including the changes. This means entering all of the schedule parameters, both those that are changing and those that are not.

Syntax

```
config firewall schedule onetime
edit <name_str>
set color <color_int>
set end <hh:mm> <yyyy/mm/dd>
set start <hh:mm> <yyyy/mm/dd>
set expiration-days <days_int>
end
```

| Variable | Description | Default |
|-------------------------------|---|---------------------|
| <name_str> | Enter the name of this schedule. | No default. |
| color <color_int> | Set the icon color to use in the web-based manager. 0 sets the default, color 1.  | 0 |
| end <hh:mm> <yyyy/mm/dd> | Enter the ending day and time of the schedule. <ul style="list-style-type: none"> • hh - 00 to 23 • mm - 00, 15, 30, or 45 • yyyy - 1992 to infinity • mm - 01 to 12 • dd - 01 to 31 | 00:00 2001/01/01 |
| start <hh:mm> <yyyy/mm/dd> | Enter the starting day and time of the schedule. <ul style="list-style-type: none"> • hh - 00 to 23 • mm - 00, 15, 30, or 45 • yyyy - 1992 to infinity • mm - 01 to 12 • dd - 01 to 31 | 00:00 2001/01/01 |
| expiration-days <days_int> | Generate an event log <days_int> days before the schedule expires. Range 1-100 days, 0 disables log. | 3 |

schedule recurring

Use this command to add, edit, and delete recurring schedules used in firewall policies.

Use scheduling to control when policies are active or inactive. Use recurring schedules to create policies that repeat weekly. Use recurring schedules to create policies that are effective only at specified times of the day or on specified days of the week.



If a recurring schedule is created with a stop time that occurs before the start time, the schedule starts at the start time and finishes at the stop time on the next day. You can use this technique to create recurring schedules that run from one day to the next. To create a recurring schedule that runs for 24 hours, set the start and stop times to the same time.

Syntax

```
config firewall schedule recurring
edit <name_str>
set day <name_str>
set end <hh:mm>
set start <hh:mm>
set color <color_int>
end
```

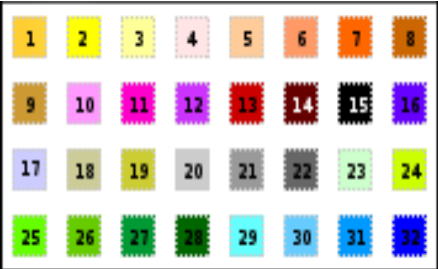
| Variable | Description | Default |
|-------------------|---|-------------|
| <name_str> | Enter the name of this schedule. | No default. |
| day <name_str> | Enter the names of one or more days of the week for which the schedule is valid. Separate multiple names with a space. | sunday |
| end <hh:mm> | Enter the ending time of the schedule. <ul style="list-style-type: none"> hh can be 00 to 23 mm can be 00, 15, 30, or 45 only | 00:00 |
| start <hh:mm> | Enter the starting time of the schedule. <ul style="list-style-type: none"> hh can be 00 to 23 mm can be 00, 15, 30, or 45 only | 00:00 |
| color <color_int> | Set the icon color to use in the web-based manager. 0 sets the default, color 1. <div data-bbox="716 1472 1138 1736" data-label="Image"> </div> | 0 |

schedule group

Use this command to configure schedule groups.

Syntax

```
config firewall schedule group
edit <group-name_str>
    set member {<schedule1_name> [schedule2_name ...]}
    set color <color_int>
end
```

| Variable | Description | Default |
|--|---|-------------|
| <group-name_str> | Enter the name of this schedule group. | No default. |
| member {<schedule1_name> [schedule2_name ...]} | Enter one or more names of one-time or recurring firewall schedules to add to the schedule group. Separate multiple names with a space. To view the list of available schedules enter <code>set member ?</code> at the prompt. Schedule names are case-sensitive. | No default. |
| color <color_int> | Set the icon color to use in the web-based manager. 0 sets the default, color 1.  | 0 |

service category

Use this command to create new categories or add comments to firewall service categories. To assign services to categories, use the `firewall service custom` command.

Syntax

```
config firewall service category
  edit <category_name>
    set comment <comment_str>
  end
```

| Variable | Description | Default |
|--------------------------|--|-------------|
| <category_name> | Predefined categories are General, Web Access, File Access, Email, Network Services, Authentication, Remote Access, Tunneling, VoIP, Messaging\ &\ Other Applications, Web Proxy Note: when entering a category name that includes spaces, escape the spaces. For example, enter “Web Access” as “Web\ Access”. | No default. |
| comment <comment_str> | | No default. |

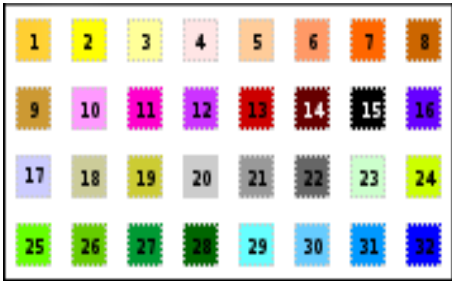
service custom

Use this command to configure firewall services.

Syntax

```
config firewall service custom
edit <name_str>
    set check-reset-range {disable | strict | default}
    set category <category_name>
    set color <color_int>
    set comment <string>
    set explicit-proxy {enable | disable}
    set fqdn <fqdn_str>
    set icmpcode <code_int>
    set icmptype <type_int>
    set iprange <serv_ip[-serv_ip]>
    set protocol {ICMP | ICMP6 | IP | TCP/UDP/SCTP}
    set protocol-number <protocol_int>
    set sctp-portrange <dstportlow_int>[-<dstporthigh_int>:
        <srcportlow_int>-<srcporthigh_int>]
    set session-ttl <seconds>
    set tcp-halfclose-timer <seconds>
    set tcp-halfopen-timer <seconds>
    set tcp-portrange <dstportlow_int>[-<dstporthigh_int>:
        <srcportlow_int>-<srcporthigh_int>]
    set tcp-timewait-timer <seconds_int>
    set udp-idle-timer <seconds>
    set udp-portrange <dstportlow_int>[-<dstporthigh_int>:
        <srcportlow_int>-<srcporthigh_int>]
    set visibility {enable | disable}
end
```

| Variable | Description | Default |
|-----------------------------|---|---------------------|
| <name_str> | Enter the name of this custom service. | No default |
| category <category_name> | Assign the service to a service category. | Depends on service. |

| Variable | Description | Default |
|--|---|-------------|
| check-reset-range {disable strict default} | <p>Configure ICMP error message verification.</p> <ul style="list-style-type: none"> disable — The FortiGate unit does not validate ICMP error messages. strict — If the FortiGate unit receives an ICMP error packet that contains an embedded IP(A,B) TCP(C,D) header, then if FortiOS can locate the A:C->B:D session it checks to make sure that the sequence number in the TCP header is within the range recorded in the session. If the sequence number is not in range then the ICMP packet is dropped. If “log-invalid-packet {enable disable}” on page 298 is enabled the FortiGate unit logs that the ICMP packet was dropped. Strict checking also affects how the anti-replay option checks packets. default — Use the global setting defined in <code>system global</code>. <p>This field is available when <code>protocol</code> is TCP/UDP/SCTP.</p> <p>This field is not available if <code>explicit-proxy</code> is enabled.</p> | default |
| color <color_int> | <p>Set the icon color to use in the web-based manager.</p> <p>0 sets the default, color 1.</p>  | 0 |
| comment <string> | Add comments for the custom service. | No default. |
| explicit-proxy {enable disable} | Enable to configure this service as an explicit web proxy service. The service will be available to explicit proxy firewall policies but not to regular firewall policies. | disable |
| fqdn <fqdn_str> | Enter a fully-qualified domain name (FQDN) for this service. | No default. |
| icmpcode <code_int> | Enter the ICMP code number. Find ICMP type and code numbers at www.iana.org . | No default. |
| icmptype <type_int> | Enter the ICMP type number. The range for <code>type_int</code> is from 0-255. Find ICMP type and code numbers at www.iana.org . | 0 |
| iprange <serv_ip[-serv_ip]> | Enter an IP address or address range for this service. | No default. |
| protocol {ICMP ICMP6 IP TCP/UDP/SCTP} | <p>Select the protocol used by the service. These protocols are available when <code>explicit-proxy</code> is disabled.</p> <p>If you select TCP/UDP/SCTP you must specify the <code>tcp-portrange</code>, <code>udp-portrange</code>, or <code>sctp-portrange</code>.</p> | IP |

| Variable | Description | Default |
|--|--|-------------|
| protocol { ALL CONNECT FTP HTTP SOCKS } | Select the protocol used by the service. These protocols are available when <code>explicit-proxy</code> is enabled. | ALL |
| protocol-number <protocol_int> | For an IP service, enter the IP protocol number. For information on protocol numbers, see http://www.iana.org . | 0 |
| sctp-portrange <dstportlow_int>[- <dstporthigh_int>: <srcportlow_int>[- <srcporthigh_int>] | For SCTP services, enter the destination and source port ranges. If the destination port range can be any port, enter 0-65535. If the destination is only a single port, simply enter a single port number for <code>dstportlow_int</code> and no value for <code>dstporthigh_int</code> . If source port can be any port, no source port need be added. If the source port is only a single port, simply enter a single port number for <code>srcportlow_int</code> and no value for <code>srcporthigh_int</code> . The total number of TCP, UDP, and SCTP port ranges cannot exceed 16. | No default. |
| session-ttl <seconds> | Enter the default session timeout in seconds. The valid range is from 300 - 604 800 seconds. Enter 0 to use either the per-policy session-ttl or per-VDOM session-ttl, as applicable. This is available when <code>protocol</code> is TCP/UDP/SCTP. | 0 |
| tcp-halfclose-timer <seconds> | Enter how many seconds the FortiGate unit should wait to close a session after one peer has sent a FIN packet but the other has not responded. The valid range is from 1 to 86400 seconds. Enter 0 to use the global setting defined in <code>system global</code> . This is available when <code>protocol</code> is TCP/UDP/SCTP. | 0 |
| tcp-halfopen-timer <seconds> | Enter how many seconds the FortiGate unit should wait to close a session after one peer has sent an open session packet but the other has not responded. The valid range is from 1 to 86400 seconds. Enter 0 to use the global setting defined in <code>system global</code> . This is available when <code>protocol</code> is TCP/UDP/SCTP. | 0 |

| Variable | Description | Default |
|--|--|-------------|
| tcp-portrange <dstportlow_int>[- <dstporthigh_int>: <srcportlow_int>- <srcporthigh_int>] | <p>For TCP services, enter the destination and source port ranges.</p> <p>If the destination port range can be any port, enter 0-65535. If the destination is only a single port, simply enter a single port number for <code>dstportlow_int</code> and no value for <code>dstporthigh_int</code>.</p> <p>If source port can be any port, no source port need be added. If the source port is only a single port, simply enter a single port number for <code>srcportlow_int</code> and no value for <code>srcporthigh_int</code>.</p> <p>The total number of TCP, UDP, and SCTP port ranges cannot exceed 16.</p> | 0:0 |
| tcp-timewait-timer <seconds_int> | <p>Set the length of the TCP TIME-WAIT state in seconds. As described in RFC 793, the “TIME-WAIT state represents waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request”.</p> <p>Reducing the time of the TIME-WAIT state means the FortiGate unit can close terminated sessions faster which means more new sessions can be opened before the session limit is reached.</p> <p>The valid range is 0 to 300 seconds. A value of 0 sets the TCP TIME-WAIT to 0 seconds</p> <p>Enter 0 to use the global setting defined in <code>system global</code>.</p> <p>This is available when <code>protocol</code> is TCP/UDP/SCTP.</p> | 1 |
| udp-idle-timer <seconds> | <p>Enter the number of seconds before an idle UDP connection times out. The valid range is from 1 to 86400 seconds.</p> <p>Enter 0 to use the global setting defined in <code>system global</code>.</p> <p>This is available when <code>protocol</code> is TCP/UDP/SCTP.</p> | 0 |
| udp-portrange <dstportlow_int>[- <dstporthigh_int>: <srcportlow_int>- <srcporthigh_int>] | <p>For UDP services, enter the destination and source port ranges.</p> <p>If the destination port range can be any port, enter 0-65535. If the destination is only a single port, simply enter a single port number for <code>dstportlow_int</code> and no value for <code>dstporthigh_int</code>.</p> <p>If source port can be any port, no source port need be added. If the source port is only a single port, simply enter a single port number for <code>srcportlow_int</code> and no value for <code>srcporthigh_int</code>.</p> <p>The total number of TCP, UDP, and SCTP port ranges cannot exceed 16.</p> | No default. |
| visibility {enable disable} | Enable visibility to include this service in firewall policy service selection. | enable |

service group

Use this command to configure firewall service groups.


To simplify policy creation, you can create groups of services and then add one policy to provide or block access for all the services in the group. A service group can contain predefined services and custom services in any combination. A service group cannot contain another service group.



To edit a service group, enter all of the members of the service group, both those changing and those staying the same.

Syntax

```
config firewall service group
edit <group-name_str>
set comment
set explicit-proxy {enable | disable}
set member <service_str>
set color <color_int>
end
```

| Variable | Description | Default |
|--------------------------------------|--|-------------|
| <group-name_str> | Enter the name of this service group. | No default. |
| comment | Add comments for this service group | No default. |
| explicit-proxy {enable disable} | Enable to configure this service group as explicit web proxy services. The service group will be available to explicit proxy firewall policies but not to regular firewall policies. | disable |
| member <service_str> | Enter one or more names of predefined or custom firewall services to add to the service group. Separate multiple names with a space. To view the list of available services enter <code>set member ?</code> at the prompt. <service_str> is case-sensitive. | No default. |
| color <color_int> | Set the icon color to use in the web-based manager. 0 sets the default, color 1.  | 0 |

shaper per-ip-shaper

Use this command to configure traffic shaping that is applied per IP address, instead of per policy or per shaper. As with the shared traffic shaper, you select per-IP traffic shapers in firewall policies.

Syntax

```
config firewall shaper per-ip-shaper
  edit <name_str>
    set diffserv-forward {enable | disable}
    set diffserv-reverse {enable | disable}
    set diffservcode-forward <dscp_bin>
    set diffservcode-rev <dscp_bin>
    set max-bandwidth <kbps_int>
    set max-concurrent-session <sessions_int>
  end
```

| Variable | Description | Default |
|--|---|-------------|
| edit <name_str> | Enter the name of the traffic shaper. | No default. |
| diffserv-forward {enable disable} | Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of forward (original) traffic. If enabled, also configure diffservcode-forward. | disable |
| diffserv-reverse {enable disable} | Enable or disable application of the differentiated services code point (DSCP) value to the DSCP field of reverse (reply) traffic. If enabled, also configure diffservcode-rev. | disable |
| diffservcode-forward <dscp_bin> | Enter the differentiated services code point (DSCP) value that the FortiGate unit will apply to the field of originating (forward) packets. The value is 6 bits binary. The valid range is 000000-111111. This option appears only if diffserv-forward is set to enable. For details and DSCP configuration examples, see the Knowledge Center article Differentiated Services Code Point (DSCP) behavior . | 000000 |
| diffservcode-rev <dscp_bin> | Enter the differentiated services code point (DSCP) value that the FortiGate unit will apply to the field of reply (reverse) packets. The value is 6 bits binary. The valid range is 000000-111111. This option appears only if diffserv-rev is set to enable For details and DSCP configuration examples, see the Knowledge Center article Differentiated Services Code Point (DSCP) behavior . | 000000 |

| Variable | Description | Default |
|--|--|---------|
| max-bandwidth <kbps_int> | Enter the maximum amount of bandwidth available for an IP address controlled by the policy. <code>Kbps_int</code> can be 0 to 16 776 000 Kbits/second. If maximum bandwidth is set to 0 no traffic is allowed by the policy. | 0 |
| max-concurrent-session <sessions_int> | Enter the maximum number of sessions allowed for an IP address. <code>sessions_int</code> can be 0 to 2097000. If maximum concurrent sessions is 0 then no sessions are allowed. | 0 |

shaper traffic-shaper

Use this command to configure shared traffic shaping that is applied to and shared by all traffic accepted by a firewall policy. As with the per-IP traffic shaper, you select shared traffic shapers in firewall policies.

Syntax

```
config firewall shaper traffic-shaper
  edit <name_str>
    set diffserv {enable | disable}
    set diffservcode <binary>
    set guaranteed-bandwidth <bandwidth_value>
    set maximum-bandwidth <bandwidth_value>
    set per-policy {enable | disable}
    set priority {high | low | medium}
  end
end
```

| Variable | Description | Default |
|---|--|-------------|
| edit <name_str> | Enter the name of the traffic shaper. | No default. |
| diffserv {enable disable} | Enable to start differentiated services on network traffic. DiffServ enables classifying network traffic and quality of service (QoS) guarantees on IP networks. | disable |
| diffservcode <binary> | Enter a 6 digit differentiate services code point (DSCP) binary code to match in the header of traffic to classify traffic. This code will be used to match traffic for this traffic shaper. | 000000 |
| guaranteed-bandwidth <bandwidth_value> | Enter the amount of bandwidth guaranteed to be available for traffic controlled by the policy. bandwidth_value can be 0 to 16 776 000 Kbits/second. | 0 |
| maximum-bandwidth <bandwidth_value> | Enter the maximum amount of bandwidth available for traffic controlled by the policy. bandwidth_value can be 0 to 16 776 000 Kbits/second. If maximum bandwidth is set to 0 no traffic is allowed by the policy. | 0 |
| per-policy {enable disable} | Enable or disable applying this traffic shaper to a single firewall policy that uses it. | disable |
| priority {high low medium} | Select the priority level for traffic controlled by the policy. | high |

sniffer

Use this command to configure sniffer policies.

Syntax

```
config firewall sniffer
  edit <policy_id>
    set application-list-status {enable | disable}
    set application_list <app_list_str>
    set av-profile-status {enable | disable}
    set av-profile <string>
    set client-reputation {enable | disable}
    set dlp-sensor-status {enable | disable}
    set dlp-sensor <string>
    set dstaddr <dstaddr_ipv4>
    set interface <int_str>
    set ips-dos-sensor {enable | disable}
    set ips-sensor-status {enable | disable}
    set ips-sensor <sensor_str>
    set ipv6 {enable | disable}
    set logtraffic {all | utm | disable}
    set logtraffic-app {enable | disable}
    set max-packet-count <int>
    set non-ip {enable | disable}
    set protocol <protocol_list>
    set srcaddr <srcaddr_ipv4>
    set status {enable | disable}
    set vlan <vlan_list>
    set webfilter-profile-status {enable | disable}
    set webfilter-profile <string>
  config anomaly
    edit <anomaly_str>
      set status {enable | disable}
      set log {enable | disable}
      set action {block | pass}
      set quarantine {attacker | both | interface | none}
      set quarantine-log {enable | disable}
      set threshold <threshold_int>
    end
  end
end
```

| Variable | Description | Default |
|---|--|---------|
| application-list-status {enable disable} | Enable to have the FortiGate unit apply an application black/white list to matching network traffic. | disable |
| application_list <app_list_str> | Enter the name of the application black/white list the FortiGate unit uses when examining network traffic. This option is available only when application-list-status is set to enable. | |

| Variable | Description | Default |
|--|---|---------|
| av-profile-status { enable disable } | Enable to have the FortiGate unit examine network traffic for virus signatures. | disable |
| av-profile <string> | Select a configured antivirus profile from the list. This option is available only when av-profile-status is enabled. | |
| client-reputation { enable disable } | Enable or disable the client reputation feature in this sniffer. | disable |
| dlp-sensor-status { enable disable } | Enable to have the FortiGate unit examine network traffic for data leaks. | disable |
| dlp-sensor <string> | Select one of the configured DLP sensors. This option is only available when dlp-sensor-status is enabled. | |
| dstaddr <dstaddr_ipv4> | Enter an address or address range to limit traffic monitoring to network traffic sent to the specified address or range. | |
| interface <int_str> | The interface or zone to be monitored. | |
| ips-dos-sensor { enable disable } | Enable to have the FortiGate unit examine network traffic for DoS sensor violations. | disable |
| ips-sensor-status { enable disable } | Enable to have the FortiGate unit examine network traffic for attacks and vulnerabilities. | disable |
| ips-sensor <sensor_str> | Enter the name of the IPS sensor the FortiGate unit will use when examining network traffic. This option is available only when ips-sensor-status is set to enable. | |
| ipv6 { enable disable } | Enable to sniff IPv6 packets. | disable |
| logtraffic { all utm disable } | Choose which traffic logs will be recorded: <ul style="list-style-type: none"> all utm - only UTM-related logs disable - no logging | utm |
| logtraffic-app { enable disable } | Enable to log traffic while application logging is active. | enable |
| max-packet-count <int> | Enter the maximum number of packets to capture when sniffing. Range 1 to 10 000. | 4000 |
| non-ip { enable disable } | Enable to sniff non-IP traffic. | disable |
| protocol <protocol_list> | Enter the protocols to sniff. | Null |
| srcaddr <srcaddr_ipv4> | Enter an address or address range to limit traffic monitoring to network traffic sent from the specified address or range. | |
| status { enable disable } | Enable or disable the sniffer policy. A disabled sniffer policy has no effect on network traffic. | enable |
| vlan <vlan_list> | Enter the VLANs to sniff. | Null |
| webfilter-profile-status { enable disable } | Enable to filter web traffic based on the selected profile. | disable |
| webfilter-profile <string> | Select a webfilter profile from the list. This options is available only when webfilter-profile-status is enabled. | |

| Variable | Description | Default |
|---|---|-------------------|
| config anomaly fields | | |
| <anomaly_str> | Enter the name of the anomaly you want to configure. Display a list of the available anomaly types by entering '?'. | |
| status {enable disable} | Enable or disable the specified anomaly. | disable |
| log {enable disable} | Enable or disable logging of the specified anomaly in the sniffer. | disable |
| action {block pass} | Select whether to pass or block traffic in which the anomaly is detected. | pass |
| quarantine {attacker both interface none} | <p>To prevent the attacker from continuing to attack the FortiGate unit, you can quarantine the attacker to the banned user list in one of three ways.</p> <ul style="list-style-type: none"> Enter <code>attacker</code> to block all traffic sent from the attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected. Enter <code>both</code> to block all traffic sent from the attacker's IP address to the target (victim's) IP address. Traffic from the attacker's IP address to addresses other than the victim's IP address is allowed. The attacker's and target's IP addresses are added to the banned user list as one entry. Enter <code>interface</code> to block all traffic from connecting to the FortiGate unit interface that received the attack. The interface is added to the banned user list. Enter <code>none</code> to disable adding addresses to the quarantine. | none |
| quarantine-log {enable disable} | Enable NAC quarantine logging. NAC quarantine logging is only available when <code>quarantine</code> is set something other than <code>none</code> . | disable |
| threshold <threshold_int> | Enter the number of times the specified anomaly must be detected in network traffic before the action is triggered. Range 1 to 2 147 483 647. | varies by anomaly |

sniff-interface-policy

Using this command you can add sniffer policies you can configure a FortiGate unit interface to operate as a one-arm intrusion detection system (IDS) appliance by sniffing packets for attacks without actually receiving and otherwise processing the packets.

To configure one-arm IDS, you need to configure one or more FortiGate interfaces to operated in one-arm sniffer mode using the `ips-sniffer-mode` field of the `config system interface` command to configure an interface to operate in one-arm sniffer mode. See “[system ips-sniffer-mode {enable | disable}](#)” on page 565. When you configure an interface to operate in one-arm sniffer mode it cannot be used for any other purpose. For example, you cannot add firewall policies for the interface and you cannot add the interface to a zone.



If you add VLAN interfaces to an interface configured for one-arm sniffer operation this VLAN interface also operates in one-arm sniffer mode and you can add sniffer policies for this VLAN interface.

After you have configured the interface for one-arm sniffer mode, connect the interface to a hub or to the SPAN port of a switch that is processing network traffic.

Then use the `config firewall sniff-interface-policy` command to add Sniffer policies for that FortiGate interface that include a DoS sensor, an IPS sensors, and an Application black/white list to detect attacks and other activity in the traffic that the FortiGate interface receives from the hub or switch SPAN port.

In one-arm sniffer mode, the interface receives packets accepted by sniffer mode policies only. All packets not received by sniffer mode policies are dropped. All packets received by sniffer mode policies go through IPS inspection and are dropped after then are analyzed by IPS.

One-arm IDS cannot block traffic. However, if you enable logging in the DoS and IPS sensors and the application black/white lists, the FortiGate unit records log messages for all detected attacks and applications.

The `sniff-interface-policy` command is applied to IPv4 addresses. For IPv6 addresses, use `sniff-interface-policy6` instead.

Syntax

```
config firewall sniff-interface-policy
edit <policy_id>
    set application-list-status {enable | disable}
    set application_list <app_list_str>
    set av-profile <string>
    set av-profile-status {enable | disable}
    set dlp-sensor <string>
    set dlp-sensor-status {enable | disable}
    set dstaddr <dstaddr_ipv4>
    set interface <int_str>
    set ips-sensor-status {enable | disable}
    set ips-sensor <sensor_str>
    set logtraffic {all | utm | disable}
    set logtraffic-app {enable | disable}
    set service <service_str>
    set srcaddr <srcaddr_ipv4>
```

```

set status {enable | disable}
set webfilter-profile <string>
set webfilter-profile-status {enable | disable}
end

```

| Variable | Description | Default |
|---|--|---------|
| application-list-status {enable disable} | Enable to have the FortiGate unit apply an application black/white list to matching network traffic. | disable |
| application_list <app_list_str> | Enter the name of the application black/white list the FortiGate unit uses when examining network traffic. This option is available only when application-list-status is set to enable. | |
| av-profile <string> | Select a configured antivirus profile from the list. This option is available only when av-profile-status is enabled. | |
| av-profile-status {enable disable} | Enable to have the FortiGate unit examine network traffic for virus signatures. | disable |
| dlp-sensor <string> | Select one of the configured DLP sensors. This option is only available when dlp-sensor-status is enabled. | |
| dlp-sensor-status {enable disable} | Enable to have the FortiGate unit examine network traffic for data leaks. | disable |
| dstaddr <dstaddr_ipv4> | Enter an address or address range to limit traffic monitoring to network traffic sent to the specified address or range. | |
| interface <int_str> | The interface or zone to be monitored. | |
| ips-sensor-status {enable disable} | Enable to have the FortiGate unit examine network traffic for attacks and vulnerabilities. | disable |
| ips-sensor <sensor_str> | Enter the name of the IPS sensor the FortiGate unit will use when examining network traffic. This option is available only when ips-sensor-status is set to enable. | |
| logtraffic {all utm disable} | Choose which traffic logs will be recorded: <ul style="list-style-type: none">allutm - only UTM-related logsdisable - no logging | utm |
| logtraffic-app {enable disable} | Enable to log traffic while application logging is active. | enable |
| service <service_str> | Enter a service to limit traffic monitoring to only the selected type. You may also specify a service group, or multiple services separated by spaces. | |
| srcaddr <srcaddr_ipv4> | Enter an address or address range to limit traffic monitoring to network traffic sent from the specified address or range. | |
| status {enable disable} | Enable or disable the sniffer policy. A disabled sniffer policy has no effect on network traffic. | enable |

| Variable | Description | Default |
|--|---|---------|
| webfilter-profile <string> | Select a webfilter profile from the list. This options is available only when webfilter-profile-status is enabled. | |
| webfilter-profile-status {enable disable} | Enable to filter web traffic based on the selected profile. | disable |

sniff-interface-policy6

Using this command you can add sniffer policies you can configure a FortiGate unit interface to operate as a one-arm intrusion detection system (IDS) appliance for IPv6 traffic by sniffing packets for attacks without actually receiving and otherwise processing the packets.

To configure one-arm IDS, you need to configure one or more FortiGate interfaces to operated in one-arm sniffer mode using the `ips-sniffer-mode` field of the `config system interface` command to configure an interface to operate in one-arm sniffer mode. See “[system ips-sniffer-mode {enable | disable}](#)” on page 565 When you configure an interface to operate in one-arm sniffer mode it cannot be used for any other purpose. For example, you cannot add firewall policies for the interface and you cannot add the interface to a zone.



If you add VLAN interfaces to an interface configured for one-arm sniffer operation this VLAN interface also operates in one-arm sniffer mode and you can add sniffer policies for this VLAN interface.

After you have configured the interface for one-arm sniffer mode, connect the interface to a hub or to the SPAN port of a switch that is processing network traffic.

Then use the `config firewall sniff-interface-policy` command to add Sniffer policies for that FortiGate interface that include a DoS sensor, an IPS sensors, and an Application black/white list to detect attacks and other activity in the traffic that the FortiGate interface receives from the hub or switch SPAN port.

In one-arm sniffer mode, the interface receives packets accepted by sniffer mode policies only. All packets not received by sniffer mode policies are dropped. All packets received by sniffer mode policies go through IPS inspection and are dropped after then are analyzed by IPS.

One-arm IDS cannot block traffic. However, if you enable logging in the IPS sensors and the application black/white lists, the FortiGate unit records log messages for all detected attacks and applications.

The `interface-policy6` command is used for DoS policies applied to IPv6 addresses. For IPv4 addresses, use `interface-policy` instead.

Syntax

```

config firewall sniff-interface-policy6
edit <policy_id>
    set application-list-status {enable | disable}
    set application_list <app_list_str>
    set av-profile <string>
    set av-profile-status {enable | disable}
    set dlp-sensor <string>
    set dlp-sensor-status {enable | disable}
    set dstaddr6 <dstaddr_ipv6>
    set interface
    set ips-sensor-status {enable | disable}
    set ips-sensor <sensor_str>
    set logtraffic {all | utm | disable}
    set logtraffic-app {enable | disable}
    set service6 <service_str>
    set srcaddr6 <srcaddr_ipv6>
    set status {enable | disable}
    set webfilter-profile <string>
    set webfilter-profile-status {enable | disable}
end

```

| Variable | Description | Default |
|---|--|---------|
| application-list-status {enable disable} | Enable to have the FortiGate unit apply an application black/white list to matching network traffic. | disable |
| application_list <app_list_str> | Enter the name of the application black/white list the FortiGate unit uses when examining network traffic. This option is available only when application-list-status is set to enable. | |
| av-profile <string> | Select a configured antivirus profile from the list. This option is available only when av-profile-status is enabled. | |
| av-profile-status {enable disable} | Enable to have the FortiGate unit examine network traffic for virus signatures. | disable |
| dlp-sensor <string> | Select one of the configured DLP sensors. This option is only available when dlp-sensor-status is enabled. | |
| dlp-sensor-status {enable disable} | Enable to have the FortiGate unit examine network traffic for data leaks. | disable |
| dstaddr6 <dstaddr_ipv6> | Enter an address or address range to limit traffic monitoring to network traffic sent to the specified address or range. | |
| interface | The interface or zone to be monitored. | |
| ips-sensor-status {enable disable} | Enable to have the FortiGate unit examine network traffic for attacks and vulnerabilities. | disable |
| ips-sensor <sensor_str> | Enter the name of the IPS sensor the FortiGate unit will use when examining network traffic. This option is available only when ips-sensor-status is set to enable. | |

| Variable | Description | Default |
|---|--|---------|
| logtraffic {all utm disable} | Choose which traffic logs will be recorded: <ul style="list-style-type: none"> all utm - only UTM-related logs disable - no logging | utm |
| logtraffic-app {enable disable} | Enable to log the application for the traffic. | enable |
| service6 <service_str> | Enter a service to limit traffic monitoring to only the selected type. You may also specify a service group, or multiple services separated by spaces. | |
| srcaddr6 <srcaddr_ipv6> | Enter an address or address range to limit traffic monitoring to network traffic sent from the specified address or range. | |
| status {enable disable} | Enable or disable the DoS policy. A disabled DoS policy has no effect on network traffic. | enable |
| webfilter-profile <string> | Select a webfilter profile from the list. This options is available only when webfilter-profile-status is enabled. | |
| webfilter-profile-status {enable disable} | Enable to filter web traffic based on the selected profile. | disable |

ssl setting

Use this command to configure SSL proxy settings so that you can apply antivirus scanning, web filtering, FortiGuard web filtering, spam filtering, data leak prevention (DLP), and content archiving to HTTPS, IMAPS, POP3S, and SMTPS traffic by using the `config firewall profile` command.

To perform SSL content scanning and inspection, the FortiGate unit does the following:

- intercepts and decrypts HTTPS, IMAPS, POP3S, and SMTPS sessions between clients and servers (FortiGate SSL acceleration speeds up decryption)
- applies content inspection to decrypted content, including:
 - HTTPS, IMAPS, POP3S, and SMTPS Antivirus, DLP, and content archiving
 - HTTPS web filtering and FortiGuard web filtering
 - IMAPS, POP3S, and SMTPS spam filtering
 - re-encrypts the sessions and forwards them to their destinations.

Syntax

```
config firewall ssl setting
    set cert-cache-capacity <capacity_integer>
    set cert-cache-timeout <timeout_integer>
    set no-matching-cipher-action {bypass | drop}
    set proxy-connect-timeout <timeout_integer>
    set session-cache-capacity <capacity_integer>
    set session-cache-timeout <port_int>
    set ssl-dh-bits {1024 | 1536 | 2048 | 768}
    set ssl-send-empty-frags {enable | disable}
end
```

| Variable | Description | Default |
|--|--|---------|
| cert-cache-capacity <capacity_integer> | Enter the capacity of the host certificate cache. The range is from 0 to 200. | 100 |
| cert-cache-timeout <timeout_integer> | Enter the time limit to keep the certificate cache. The range is from 1 to 120 minutes. | 10 |
| no-matching-cipher-action {bypass drop} | Bypass or drop SSL traffic when unsupported cipher is being used by the server. | bypass |
| proxy-connect-timeout <timeout_integer> | Enter the time limit to make an internal connection to the appropriate proxy process (1 - 60 seconds). | 30 |
| session-cache-capacity <capacity_integer> | Enter the capacity of SSL session cache (0 - 1000). | 500 |
| session-cache-timeout <port_int> | Enter the time limit in minutes to keep the SSL session. | 20 |
| ssl-dh-bits {1024 1536 2048 768} | Select the size of Diffie-Hellman prime used in DHE_RSA negotiation. | 1024 |
| ssl-send-empty-frags {enable disable} | Enable or disable sending empty fragments to avoid attack on CBC IV (SSL 3.0 & TLS 1.0 only). | enable |

ttl-policy

Use this command to create Generalized TTL Security Mechanism (GTSM) policies.

Syntax

```
config firewall ttl-policy
edit <id>
    set action {accept | deny}
    set schedule <name_str>
    set service <name_str>
    set srcaddr <name_str>
    set srcintf <name_str>
    set status {enable | disable}
    set ttl <ttl-range>
end
```

| Variable | Description | Value |
|---------------------------|---|-------------|
| action {accept deny} | | |
| schedule <name_str> | Enter the name of the one-time or recurring schedule or schedule group to use for the policy. | No default. |
| service <name_str> | Enter the name of one or more services, or a service group, to match with the firewall policy. Separate multiple services with a space. | No default. |
| srcaddr <name_str> | Enter one or more source firewall addresses for the policy. Separate multiple firewall addresses with a space. | No default. |
| srcintf <name_str> | Enter the source interface for the policy. | No default. |
| status {enable disable} | Enable or disable this policy. | enable |
| ttl <ttl-range> | Enter the range of TTL values to match in the form low-high, "253-255" for example. | null |

vip

Use this command to configure virtual IPs and their associated address and port mappings (NAT).

Virtual IPs can be used to allow connections through a FortiGate unit using network address translation (NAT) firewall policies. Virtual IPs can use proxy ARP so that the FortiGate unit can respond to ARP requests on a network for a server that is actually installed on another network. Proxy ARP is defined in RFC 1027.

For example, you can add a virtual IP to an external FortiGate unit interface so that the external interface can respond to connection requests for users who are actually connecting to a server on the DMZ or internal network.

Depending on your configuration of the virtual IP, its mapping may involve port address translation (PAT), also known as port forwarding or network address port translation (NAPT), and/or network address translation (NAT) of IP addresses.

If you configure NAT in the virtual IP and firewall policy, the NAT behavior varies by your selection of:

- static vs. dynamic NAT mapping
- the dynamic NAT's load balancing style, if using dynamic NAT mapping
- full NAT vs. destination NAT (DNAT)

The following table describes combinations of PAT and/or NAT that are possible when configuring a firewall policy with a virtual IP.

| | |
|--|---|
| Static NAT | <p>Static, one-to-one NAT mapping: an external IP address is always translated to the same mapped IP address.</p> <p>If using IP address ranges, the external IP address range corresponds to a mapped IP address range containing an equal number of IP addresses, and each IP address in the external range is always translated to the same IP address in the mapped range.</p> |
| Static NAT with Port Forwarding | <p>Static, one-to-one NAT mapping with port forwarding: an external IP address is always translated to the same mapped IP address, and an external port number is always translated to the same mapped port number.</p> <p>If using IP address ranges, the external IP address range corresponds to a mapped IP address range containing an equal number of IP addresses, and each IP address in the external range is always translated to the same IP address in the mapped range. If using port number ranges, the external port number range corresponds to a mapped port number range containing an equal number of port numbers, and each port number in the external range is always translated to the same port number in the mapped range.</p> |
| Load Balancing | <p>Dynamic, one-to-many NAT mapping: an external IP address is translated to one of the mapped IP addresses. For each session, a load balancing algorithm dynamically selects an IP address from the mapped IP address range to provide more even traffic distribution. The external IP address is not always translated to the same mapped IP address.</p> |

| | |
|---|---|
| Load Balancing with Port Forwarding | Dynamic, one-to-many NAT mapping with port forwarding: an external IP address is translated to one of the mapped IP addresses. For each session, a load balancing algorithm dynamically selects an IP address from the mapped IP address range to provide more even traffic distribution. The external IP address is not always translated to the same mapped IP address. |
| Dynamic Virtual IPs | Dynamic, one-to-one NAT mapping for an interface with dynamically assigned IP address. If you set the external IP address of a virtual IP to 0.0.0.0, the interface maps traffic destined for the interface IP address, and is dynamically translated to a mapped IP address or address range. |
| Server Load Balancing | <p>Dynamic, one-to-many NAT mapping: an external IP address is translated to one of the mapped IP addresses, as determined by the selected load balancing algorithm for more even traffic distribution. The external IP address is not always translated to the same mapped IP address.</p> <p>Server load balancing requires that you configure at least one “real” server, but can use up to eight (8) real servers per virtual IP (VIP). Real servers can be configured with health check monitors. Health check monitors can be used to gauge server responsiveness before forwarding packets.</p> |
| Server Load Balancing with Port Forwarding | <p>Dynamic, one-to-many NAT mapping with port forwarding: an external IP address is translated to one of the mapped IP addresses, as determined by the selected load balancing algorithm for more even traffic distribution. The external IP address is not always translated to the same mapped IP address.</p> <p>Server load balancing requires that you configure at least one “real” server, but can use up to eight (8) real servers per virtual IP (VIP). Real servers can be configured with health check monitors. Health check monitors can be used to gauge server responsiveness before forwarding packets.</p> |



If the NAT check box is not selected when building the firewall policy, the resulting policy does not perform full (source and destination) NAT; instead, it performs destination network address translation (DNAT).

For inbound traffic, DNAT translates packets' destination address to the mapped private IP address, but does not translate the source address. The private network is aware of the source's public IP address. For reply traffic, the FortiGate unit translates packets' private network source IP address to match the destination address of the originating packets, which is maintained in the session table.

The following limitations apply when adding virtual IPs, Load balancing virtual servers, and load balancing real servers. Load balancing virtual servers are actually server load balancing virtual IPs. You can add server load balance virtual IPs from the CLI.

- Virtual IP `extip` entries or ranges cannot overlap with each other unless `src-filter` is used.
- A virtual IP `mappedip` cannot be 0.0.0.0 or 255.255.255.255.
- A real server IP cannot be 0.0.0.0 or 255.255.255.255.
- If a static NAT virtual IP `extip` is 0.0.0.0, the `mappedip` must be a single IP address.
- If a load balance virtual IP `extip` is 0.0.0.0, the `mappedip` can be an address range.

- When port forwarding, the count of mappedport and extport numbers must be the same. The web-based manager does this automatically but the CLI does not.
- Virtual IP names must be different from firewall address or address group names.

Syntax

```
config firewall vip
edit <name_str>
    set arp-reply {enable | disable}
    set comment <comment_str>
    set extintf <name_str>
    set extip <address_ipv4>[-<address_ipv4>]
    set extport <port_int>
    set gratuitous-arp-interval <interval_seconds>
    set http-cookie-age <age_int>
    set http-cookie-domain <domain_str>
    set http-cookie-domain-from-host {enable | disable}
    set http-cookie-generation <generation_int>
    set http-cookie-path <path_str>
    set http-cookie-share {disable | same-ip}
    set http-ip-header {enable | disable}
    set http-multiplex {enable | disable}
    set https-cookie-secure {disable | enable}
    set id <id_num_str>
    set ldb-method {first-alive | http-host | least-rtt
        | least-session | round-robin | static | weighted}
    set mappedip [<start_ipv4>-<end_ipv4>]
    set mappedport <port_int>
    set max-embryonic-connections <initiated_int>
    set monitor <name_str>
    set nat-source-vip {enable | disable}
    set outlook-web-access {disable | enable}
    set persistence {none | ssl-session-id | http-cookie(http)}
    set portforward {enable | disable}
    set portmapping-type {1-to-1 | m-to-n}
    set protocol {sctp | tcp | udp}
    set server-type {http | https | imaps | ip | pop3s | smtps | ssl
        | tcp | udp}
    set src-filter <addr_str>
    set srcintf-filter <intf_str>
    set ssl-mode {full | half}
    set ssl-algorithm {low | medium | high | custom}
    set ssl-certificate <certificate_str>
    set ssl-client-renegotiation {allow | deny | secure}
    set ssl-client-session-state-max <sessionstates_int>
    set ssl-client-session-state-timeout <timeout_int>
    set ssl-client-session-state-type {both | client | disable |
        time}
    set ssl-dh-bits <bits_int>
    set ssl-http-location-conversion {enable | disable}
```



```

set ssl-http-match-host {enable | disable}?
set ssl-max-version {ssl-3.0 | tls-1.0}
set ssl-min-version {ssl-3.0 | tls-1.0}
set ssl-pfs {allow | deny | require}
set ssl-send-empty-frags {enable | disable}
set ssl-server-session-state-max <sessionstates_int>
set ssl-server-session-state-timeout <timeout_int>
set ssl-server-session-state-type {both | count | disable |
    time}
set type {load-balance | server-load-balance | static-nat}
set weblogic-server {enable | disable}
set websphere-server {enable | disable}
config realservers
    edit <table_id>
        set client-ip <ip_range_ipv4> [<ip_range_ipv4>]
            [<ip_range_ipv4>] [<ip_range_ipv4>]
        set healthcheck {enable | disable}
        set holddown-interval <seconds_int>
        set http-host <host_str>
        set ip <server_ip>
        set max-connections <connection_integer>
        set monitor <healthcheck_str>
        set port <port_ip>
        set status {active | disable | standby}
        set weight <loadbalanceweight_int>
    end
config ssl-cipher-suites
    edit <id>
        set cipher <cipher_name>
        set versions {ssl-3.0 tls-1.0 tls-1.1}
    end
end

```

| Variable | Description | Default |
|---------------------------------|---|-------------|
| <name_str> | Enter the name of this virtual IP address. | No default. |
| arp-reply {enable disable} | Select to respond to ARP requests for this virtual IP address. | enable |
| comment <comment_str> | Enter comments relevant to the configured virtual IP. | No default |
| extintf <name_str> | Enter the name of the interface connected to the source network that receives the packets that will be forwarded to the destination network. The interface name can be any FortiGate network interface, VLAN subinterface, IPSec VPN interface, or modem interface. | No default. |

| Variable | Description | Default |
|--|---|---------|
| extip <address_ipv4>[-<address_ipv4>] | <p>Enter the IP address or address range on the external interface that you want to map to an address or address range on the destination network.</p> <p>If type is static-nat and mappedip is an IP address range, the FortiGate unit uses extip as the first IP address in the external IP address range, and calculates the last IP address required to create an equal number of external and mapped IP addresses for one-to-one mapping.</p> <p>To configure a dynamic virtual IP that accepts connections destined for any IP address, set extip to 0.0.0.0.</p> | 0.0.0.0 |
| extport <port_int> | <p>Enter the external port number that you want to map to a port number on the destination network.</p> <p>This option only appears if portforward is enabled.</p> <p>If portforward is enabled and you want to configure a static NAT virtual IP that maps a range of external port numbers to a range of destination port numbers, set extport to the first port number in the range. Then set mappedport to the start and end of the destination port range. The FortiGate unit automatically calculates the end of the extport port number range.</p> <p>If type is server-load-balance, extport is available unless server-type is ip. The value of extport changes to 80 if server-type is http and to 443 if server-type is https.</p> | 0 |
| gratuitous-arp-interval <interval_seconds> | Configure sending of ARP packets by a virtual IP. You can set the time interval between sending ARP packets. Set the interval to 0 to disable sending ARP packets. | 0 |
| http-cookie-age <age_int> | <p>Configure HTTP cookie persistence to change how long the browser caches the cookie. Enter an age in minutes or set the age to 0 to make the browser keep the cookie indefinitely. The range is 0 to 525600 minutes.</p> <p>This option is available when type is server-load-balance, server-type is http or https and persistence is http or https.</p> | 60 |
| http-cookie-domain <domain_str> | <p>Configure HTTP cookie persistence to restrict the domain that the cookie should apply to. Enter the DNS domain name to restrict the cookie to.</p> <p>This option is available when type is server-load-balance, server-type is http or https and persistence is http or https.</p> | |

| Variable | Description | Default |
|---|---|---------|
| http-cookie-domain-from-host {enable disable} | <p>If enabled, when the FortiGate unit adds a SetCookie to the HTTP(S) response, the Domain attribute in the SetCookie will be set to the value of the Host: header, if there was one.</p> <p>If there was no Host: header, the Domain attribute will be set to the value of http-cookie-domain if it is set and if it is not then the Domain attribute will not be included in the SetCookie.</p> <p>This option is available when type is server-load-balance, server-type is http or https and persistence is http-cookie.</p> | disable |
| http-cookie-generation <generation_int> | <p>Configure HTTP cookie persistence to invalidate all cookies that have already been generated. The exact value of the generation is not important, only that it is different from any generation that has already been used.</p> <p>This option is available when type is server-load-balance, server-type is http or https and persistence is http or https.</p> | 0 |
| http-cookie-path <path_str> | <p>Configure HTTP cookie persistence to limit the cookies to a particular path, for example /new/path.</p> <p>This option is available when type is server-load-balance, server-type is http or https and persistence is http or https.</p> | |
| http-cookie-share {disable same-ip} | <p>Configure HTTP cookie persistence to control the sharing of cookies across more than one virtual server. The default setting same-ip means that any cookie generated by one virtual server can be used by another virtual server in the same virtual domain.</p> <p>Select disable to make sure that a cookie generated for a virtual server cannot be used by other virtual servers.</p> <p>This options is available when type is server-load-balance, server-type is http or https and persistence is http or https.</p> | same-ip |
| http-ip-header {enable disable} | <p>Select to preserve the client's IP address in the X-Forwarded-For HTTP header line if HTTP multiplexing is enabled. This can be useful if you require logging on the server of the client's original IP address. If this option is not selected, in HTTP multiplexing configurations the header will contain the IP address of the FortiGate unit.</p> <p>This option appears only if portforward and http-multiplex are enable.</p> | disable |

| Variable | Description | Default |
|---|---|-------------|
| http-multiplex {enable disable} | Select to use the FortiGate unit to multiplex multiple client connections into a few connections between the FortiGate unit and the real server. This can improve performance by reducing server overhead associated with establishing multiple connections. The server must be HTTP/1.1 compliant. This option is only available if <code>server-type</code> is <code>http</code> or <code>https</code> . | disable |
| https-cookie-secure {disable enable} | Configure HTTP cookie persistence to enable or disable using secure cookies for HTTPS sessions. Secure cookies are disabled by default because they can interfere with cookie sharing across HTTP and HTTPS virtual servers. If enabled, then the <code>Secure</code> tag is added to the cookie inserted by the FortiGate unit. This option is available when <code>type</code> is <code>server-load-balance</code> , <code>server-type</code> is <code>http</code> or <code>https</code> and <code>persistence</code> is <code>http</code> or <code>https</code> . | disable |
| id <id_num_str> | Enter a unique identification number for the configured virtual IP. Not checked for uniqueness. Range 0 - 65535. | No default. |

| Variable | Description | Default |
|--|---|---------|
| ldb-method {first-alive http-host least-rtt least-session round-robin static weighted} | <p>Select the method used by the virtual server to distribute sessions to the real servers. You add real servers to the virtual server using <code>config realservers</code>.</p> <ul style="list-style-type: none"> <code>first-alive</code>: Always directs requests to the first alive real server. In this case “first” refers to the order of the real servers in the virtual server configuration. For example, if you add real servers A, B and C in that order, then traffic always goes to A as long as it is alive. If A goes down then traffic goes to B and if B goes down the traffic goes to C. If A comes back up, traffic goes to A. Real servers are ordered in the virtual server configuration in the order in which you add them, with the most recently added real server last. If you want to change the order you must delete and re-add real servers as required. <code>http-host</code>: Load balance HTTP requests by the contents of the HOST header. <code>least-rtt</code>: Directs requests to the real server with the least round trip time. The round trip time is determined by a Ping monitor and is defaulted to 0 if no Ping monitors are defined. <code>least-session</code>: Directs requests to the real server that has the least number of current connections. This method works best in environments where the real servers or other equipment you are load balancing have similar capabilities. <code>round-robin</code>: Directs request to the next real server, and treats all real servers as equals regardless of response time or number of connections. Unresponsive real servers are avoided. A separate real server is required. <code>static</code>: Distributes sessions evenly across all real servers according to the session source IP address. This load balancing method provides some persistence because all sessions from the same source address would always go to the same server. However, the distribution is stateless, so if a real server is added or removed (or goes up or down) the distribution is changed so persistence will be lost. Separate real servers are not required. <code>weighted</code>: Real servers with a higher weight value receive a larger percentage of connections at any one time. Server weights can be set in <code>config realservers set weight</code> <p>This option appears only if type is <code>server-load-balance</code>.</p> | static |

| Variable | Description | Default |
|--|--|-------------|
| mappedip [<start_ipv4>-<end_ipv4>] | <p>Enter the IP address or IP address range on the destination network to which the external IP address is mapped.</p> <p>If type is static-nat and mappedip is an IP address range, the FortiGate unit uses extip as the first IP address in the external IP address range, and calculates the last IP address required to create an equal number of external and mapped IP addresses for one-to-one mapping.</p> <p>If type is load-balance and mappedip is an IP address range, the FortiGate unit uses extip as a single IP address to create a one-to-many mapping.</p> | 0.0.0.0 |
| mappedport <port_int> | <p>Enter the port number on the destination network to which the external port number is mapped.</p> <p>You can also enter a port number range to forward packets to multiple ports on the destination network.</p> <p>For a static NAT virtual IP, if you add a map to port range the FortiGate unit calculates the external port number range.</p> | 0 |
| max-embryonic-connections <initiated_int> | <p>Enter the maximum number of partially established SSL or HTTP connections. This should be greater than the maximum number of connections you want to establish per second.</p> <p>This option appears only if portforward is enable, and http is enable or ssl is not off.</p> | 1000 |
| monitor <name_str> | Select the health check monitor for use when polling to determine a virtual server's connectivity status. | No default. |
| nat-source-vip {enable disable} | <p>Enable to prevent unintended servers from using a virtual IP. The virtual IP will be used as the source IP address for connections from the server through the FortiGate unit.</p> <p>Disable to use the actual IP address of the server (or the FortiGate destination interface if using NAT) as the source address of connections from the server that pass through the FortiGate unit.</p> | disable |
| outlook-web-access {disable enable} | <p>If the FortiGate unit provides SSL offload for Microsoft Outlook Web Access then the Outlook server expects to see a Front-End-Https: on header inserted into the HTTP headers as described in this Microsoft Technical Note. If outlook-web-access is enabled FortiGate unit adds this header to all HTTP requests.</p> <p>This options is available when type is server-load-balance, server-type is http or https.</p> | disable |

| Variable | Description | Default |
|--|---|---------|
| <p>persistence { none ssl-session-id http-cookie(http) }</p> <p>http https ssl</p> | <p>If the type is server-load-balance, configure persistence for a virtual server to make sure that clients connect to the same server every time they make a request that is part of the same session.</p> <p>When you configure persistence, the FortiGate unit load balances a new session to a real server according to the ldb-method. If the session has an HTTP cookie or an SSL session ID, the FortiGate unit sends all subsequent sessions with the same HTTP cookie or SSL session ID to the same real server.</p> <p>You can configure persistence if server-type is set to http, https, or ssl.</p> <ul style="list-style-type: none"> • none: No persistence. Sessions are distributed solely according to the ldb-method. Setting ldb-method to static (the default) results in behavior equivalent to persistence. See the description of static in “firewall ldb-method {first-alive http-host least-rtt least-session round-robin static weighted}” on page 229 for more information. • http-cookie: all HTTP or HTTPS sessions with the same HTTP session cookie are sent to the same real server. http-cookie is available if server-type is set to https or ssl. If you select http-cookie you can also configure http-cookie-domain, http-cookie-path, http-cookie-generation, http-cookie-age, and http-cookie-share for HTTP and these settings plus https-cookie-secure for HTTPS. • ssl-session-id: all sessions with the same SSL session ID are sent to the same real server. ssl-session-id is available if server-type is set to https or ssl. | none |
| <p>portforward {enable disable}</p> | Select to enable port forwarding. You must also specify the port forwarding mappings by configuring extport and mappedport. | disable |
| <p>portmapping-type { 1-to-1 m-to-n }</p> | <p>Select the type of port mapping.</p> <p>1-to-1 — one-to-one mapping</p> <p>m-to-n — load balancing</p> <p>This is available when portforward is enable.</p> | 1-to-1 |
| <p>protocol {sctp tcp udp}</p> | Select the protocol, TCP or UDP, to use when forwarding packets. | tcp |

| Variable | Description | Default |
|---|---|---------|
| server-type {http https imaps ip pop3s smtps ssl tcp udp} | <p>If the type is <code>server-load-balance</code>, select the protocol to be load balanced by the virtual server (also called the server load balance virtual IP). If you select a general protocol such as <code>ip</code>, <code>tcp</code>, or <code>udp</code> the virtual server load balances all IP, TCP, or UDP sessions. If you select specific protocols such as <code>http</code>, <code>https</code>, or <code>ssl</code> you can apply additional server load balancing features such as persistence and HTTP multiplexing.</p> <ul style="list-style-type: none"> • <code>http</code>: load balance only HTTP sessions with destination port number that matches the <code>extport</code> setting. Change <code>extport</code> to match the destination port of the sessions to be load balanced. You can also configure <code>http-multiplex</code>. You can also set persistence to <code>http-cookie</code> and configure <code>http-cookie-domain</code>, <code>http-cookie-path</code>, <code>http-cookie-generation</code>, <code>http-cookie-age</code>, and <code>http-cookie-share</code> settings for cookie persistence. • <code>https</code>: load balance only HTTPS sessions with destination port number that matches the <code>extport</code> setting. Change <code>extport</code> to match the destination port of the sessions to be load balanced. You can also configure <code>http-multiplex</code> and set persistence to <code>http-cookie</code> and configure the same <code>http-cookie</code> options as for <code>http</code> virtual servers plus the <code>https-cookie-secure</code> option. You can also set persistence to <code>ssl-session-id</code>. You can also configure the SSL options such as <code>ssl-mode</code> and <code>ssl-certificate</code> and so on. <code>https</code> is available on FortiGate units that support SSL acceleration. • <code>imaps</code>: load balance only IMAPS sessions with destination port number that matches the <code>extport</code> setting. Change <code>extport</code> to match the destination port of the sessions to be load balanced. • <code>ip</code>: load balance all sessions accepted by the firewall policy that contains this server load balance virtual IP. Since all sessions are load balanced you don't have to set the <code>extport</code>. • <code>pop3s</code>: load balance only POP3S sessions with destination port number that matches the <code>extport</code> setting. Change <code>extport</code> to match the destination port of the sessions to be load balanced. • <code>smtps</code>: load balance only SMTPS sessions with destination port number that matches the <code>extport</code> setting. Change <code>extport</code> to match the destination port of the sessions to be load balanced. | (none) |

| Variable | Description | Default |
|--|--|-------------|
| | <ul style="list-style-type: none"> <code>ssl</code>: load balance only SSL sessions with destination port number that matches the <code>extport</code> setting. Change <code>extport</code> to match the destination port of the sessions to be load balanced. You can also configure the SSL options such as <code>ssl-mode</code> and <code>ssl-certificate</code> and so on. <code>tcp</code>: load balance only TCP sessions with destination port number that matches the <code>extport</code> setting. Change <code>extport</code> to match the destination port of the sessions to be load balanced. <code>udp</code>: load balance only UDP sessions with destination port number that matches the <code>extport</code> setting. Change <code>extport</code> to match the destination port of the sessions to be load balanced. | |
| <code>src-filter <addr_str></code> | Enter a source address filter. Each address must be either an IP/subnet (x.x.x.x/n) or a range (x.x.x.x-y.y.y.y). Separate addresses by spaces. | null |
| <code>srcintf-filter <intf_str></code> | Enter names of the interfaces to which the VIP applies. Separate names with spaces. | No default. |

| Variable | Description | Default |
|--|---|-------------|
| ssl-mode {full half} | <p>Select whether or not to accelerate SSL communications with the destination by using the FortiGate unit to perform SSL operations, and indicate which segments of the connection will receive SSL offloading. Accelerating SSL communications in this way is also called SSL offloading.</p> <ul style="list-style-type: none"> full: Select to apply SSL acceleration to both parts of the connection: the segment between the client and the FortiGate unit, and the segment between the FortiGate unit and the server. The segment between the FortiGate unit and the server will use encrypted communications, but the handshakes will be abbreviated. This results in performance which is less than the option half, but still improved over communications without SSL acceleration, and can be used in failover configurations where the failover path does not have an SSL accelerator. If the server is already configured to use SSL, this also enables SSL acceleration without requiring changes to the server's configuration. half: Select to apply SSL only to the part of the connection between the client and the FortiGate unit. The segment between the FortiGate unit and the server will use clear text communications. This results in best performance, but cannot be used in failover configurations where the failover path does not have an SSL accelerator. <p>SSL 3.0 and TLS 1.0 are supported.</p> <p>This option appears only if <code>server-type</code> is <code>ssl</code> or <code>https</code>.</p> | full |
| ssl-algorithm {low medium high custom} | <p>Set the permitted encryption algorithms for SSL sessions according to encryption strength:</p> <p>low — AES, 3DES, RC4, DES</p> <p>medium — AES, 3DES, RC4</p> <p>high — AES, 3DES</p> <p>custom — determined in config <code>ssl-cipher-suites</code> subcommand</p> | high |
| ssl-certificate <certificate_str> | <p>Enter the name of the SSL certificate to use with SSL acceleration.</p> <p>This option appears only if <code>type</code> is <code>server-load-balance</code> and <code>server-type</code> is <code>ssl</code>.</p> | No default. |

| Variable | Description | Default |
|--|--|---------|
| ssl-client-renegotiation {allow deny secure} | <p>Select the SSL secure renegotiation policy.</p> <p>allow — Allow, but do not require secure renegotiation.</p> <p>deny — Do not allow renegotiation.</p> <p>secure — Require secure renegotiation.</p> <p>Secure renegotiation complies with RFC 5746 Secure Negotiation Indication.</p> | allow |
| ssl-client-session-state-max <sessionstates_int> | <p>Enter the maximum number of SSL session states to keep for the segment of the SSL connection between the client and the FortiGate unit.</p> <p>This option appears only if type is server-load-balance and server-type is ssl.</p> | 1000 |
| ssl-client-session-state-timeout <timeout_int> | <p>Enter the number of minutes to keep the SSL session states for the segment of the SSL connection between the client and the FortiGate unit.</p> <p>This option appears only if type is server-load-balance and server-type is ssl.</p> | 30 |
| ssl-client-session-state-type {both client disable time} | <p>Select which method the FortiGate unit should use when deciding to expire SSL sessions for the segment of the SSL connection between the client and the FortiGate unit.</p> <ul style="list-style-type: none"> both: Select to expire SSL session states when either ssl-client-session-state-max or ssl-client-session-state-timeout is exceeded, regardless of which occurs first. count: Select to expire SSL session states when ssl-client-session-state-max is exceeded. disable: Select to keep no SSL session states. time: Select to expire SSL session states when ssl-client-session-state-timeout is exceeded. <p>This option appears only if type is server-load-balance and server-type is ssl.</p> | both |
| ssl-dh-bits <bits_int> | <p>Enter the number of bits of the prime number used in the Diffie-Hellman exchange for RSA encryption of the SSL connection. Larger prime numbers are associated with greater cryptographic strength.</p> <p>This option appears only if type is server-load-balance and server-type is ssl.</p> | 1024 |
| ssl-http-location-conversion {enable disable} | <p>Select to replace http with https in the reply's Location HTTP header field.</p> <p>For example, in the reply, Location: http://example.com/ would be converted to Location: https://example.com/.</p> <p>This option appears only if type is server-load-balance and server-type is https.</p> | disable |

| Variable | Description | Default |
|--|--|---------|
| ssl-http-match-host {enable disable} | <p>Select to apply <code>Location</code> conversion to the reply's HTTP header only if the host name portion of <code>Location</code> matches the request's <code>Host</code> field, or, if the <code>Host</code> field does not exist, the host name portion of the request's URI. If disabled, conversion occurs regardless of whether the host names in the request and the reply match.</p> <p>For example, if host matching is enabled, and a request contains <code>Host: example.com</code> and the reply contains <code>Location: http://example.cc/</code>, the <code>Location</code> field does not match the host of the original request and the reply's <code>Location</code> field remains unchanged. If the reply contains <code>Location: http://example.com/</code>, however, then the FortiGate unit detects the matching host name and converts the reply field to <code>Location: https://example.com/</code>.</p> <p>This option appears only if <code>ssl-http-location-conversion</code> is enable.</p> | disable |
| ssl-max-version {ssl-3.0 tls-1.0} | <p>Enter the maximum version of SSL/TLS to accept in negotiation.</p> <p>This option appears only if <code>type</code> is <code>server-load-balance</code> and <code>server-type</code> is <code>ssl</code>.</p> | tls-1.0 |
| ssl-min-version {ssl-3.0 tls-1.0} | <p>Enter the minimum version of SSL/TLS to accept in negotiation.</p> <p>This option appears only if <code>type</code> is <code>server-load-balance</code> and <code>server-type</code> is <code>ssl</code>.</p> | ssl-3.0 |
| ssl-pfs {allow deny require} | <p>Select handling of perfect forward secrecy (PFS) for connections:</p> <p><code>allow</code> — Allow use of any cipher suite.</p> <p><code>deny</code> — Allow only non-Diffie-Hellman cipher-suites.</p> <p><code>require</code> — Allow only Diffie-Hellman cipher-suites.</p> | allow |
| ssl-send-empty-frags {enable disable} | <p>Select to precede the record with empty fragments to thwart attacks on CBC IV. You might disable this option if SSL acceleration will be used with an old or buggy SSL implementation which cannot properly handle empty fragments.</p> <p>This option appears only if <code>type</code> is <code>server-load-balance</code> and <code>server-type</code> is <code>ssl</code>, and applies only to SSL 3.0 and TLS 1.0.</p> | enable |
| ssl-server-session-state-max <sessionstates_int> | <p>Enter the maximum number of SSL session states to keep for the segment of the SSL connection between the server and the FortiGate unit.</p> <p>This option appears only if <code>ssl-mode</code> is <code>full</code>.</p> | 1000 |
| ssl-server-session-state-timeout <timeout_int> | <p>Enter the number of minutes to keep the SSL session states for the segment of the SSL connection between the server and the FortiGate unit.</p> <p>This option appears only if <code>ssl-mode</code> is <code>full</code>.</p> | 30 |

| Variable | Description | Default |
|---|--|------------|
| ssl-server-session-state-type {both count disable time} | <p>Select which method the FortiGate unit should use when deciding to expire SSL sessions for the segment of the SSL connection between the server and the FortiGate unit.</p> <ul style="list-style-type: none"> both: Select to expire SSL session states when either <code>ssl-server-session-state-max</code> or <code>ssl-server-session-state-timeout</code> is exceeded, regardless of which occurs first. count: Select to expire SSL session states when <code>ssl-server-session-state-max</code> is exceeded. disable: Select to keep no SSL session states. time: Select to expire SSL session states when <code>ssl-server-session-state-timeout</code> is exceeded. <p>This option appears only if <code>ssl-mode</code> is <code>full</code>.</p> | both |
| type {load-balance server-load-balance static-nat} | <p>Select the type of static or dynamic NAT applied by the virtual IP.</p> <ul style="list-style-type: none"> load-balance: Dynamic NAT load balancing with server selection from an IP address range. server-load-balance: Dynamic NAT load balancing with server selection from among up to eight <code>realserver</code>s, determined by your selected load balancing algorithm and server responsiveness monitors. static-nat: Static NAT. | static-nat |
| weblogic-server {enable disable} | Enable or disable adding HTTP header to indicate SSL offload for WebLogic server. | disable |
| websphere-server {enable disable} | Enable or disable adding HTTP header to indicate SSL offload for WebSphere server. | disable |

| Variable | Description | Default |
|--|--|-------------|
| realservers The following are the options for <code>config realservers</code> , and are available only if <code>type</code> is <code>server-load-balance</code> . | | |
| client-ip <code><ip_range_ipv4></code> <code>[<ip_range_ipv4>]</code> <code>[<ip_range_ipv4>]</code> <code>[<ip_range_ipv4>]</code> | Restrict the clients that can connect to a real server according to the client's source IP address. Use the <code>client-ip</code> option to enter up to four client source IP addresses or address ranges. Separate each IP address or range with a space. The following example shows how to add a single IP address and an IP address range: <pre>set client-ip 192.168.1.90 192.168.1.100-192.168.1.120</pre> Use the <code>client-ip</code> option if you have multiple real servers in a server load balance VIP and you want to control which clients use which real server according to the client's source IP address. Different real servers in the same virtual server can have the same or overlapping IP addresses and ranges. If an overlap occurs, sessions from the overlapping source addresses are load balanced among the real servers with the overlapping addresses. If you do not specify a <code>client-ip</code> all clients can use the real server. | |
| <code><table_id></code> | Enter an index number used to identify the server that you are configuring. You can configure a maximum number of eight (8) servers in a server load balancing cluster. | No default. |
| healthcheck <code>{enable disable}</code> | Enable to check the responsiveness of the server before forwarding traffic. You must also configure <code>monitor</code> . | disable |

| Variable | Description | Default |
|---|---|---------|
| holddown-interval <seconds_int> | <p>Enter the amount of time in seconds that the health check monitor will continue to monitor the status of a server whose <code>status</code> is <code>active</code> after it has been detected to be unresponsive.</p> <ul style="list-style-type: none"> If the server is detected to be continuously responsive during this interval, a server whose <code>status</code> is <code>standby</code> will be removed from current use and replaced with this server, which will again be used by server load balanced traffic. In this way, server load balancing prefers to use servers whose <code>status</code> is <code>active</code>, if they are responsive. If the server is detected to be unresponsive during the first holddown interval, the server will remain out of use for server load balanced traffic, the health check monitor will double the holddown interval once, and continue to monitor the server for the duration of the doubled holddown interval. The health check monitor continues to monitor the server for additional iterations of the doubled holddown interval until connectivity to the server becomes reliable, at which time the holddown interval will revert to the configured interval, and the newly responsive server whose <code>status</code> is <code>active</code> will replace the standby server in the pool of servers currently in use. In effect, if the <code>status</code> of a server is <code>active</code> but the server is habitually unresponsive, the health check monitor is less likely to restore the server to use by server load balanced traffic until the server's connectivity becomes more reliable. <p>This option applies only to real servers whose <code>status</code> is <code>active</code>, but have been detected to be unresponsive ("down").</p> | 300 |
| http-host <host_str> | <p>Enter the value of the HOST header to match. For traffic to use the realserver, the HTTP(S) Host: header must match (case insensitive) the value of the <code>http-host</code> attribute.</p> <p>This is available when VIP <code>ldb-method</code> is <code>http-host</code>.</p> | null |
| ip <server_ip> | Enter the IP address of a server in this server load balancing cluster. | 0.0.0.0 |
| max-connections <connection_integer> | <p>Enter the limit on the number of active connections directed to a real server. If the maximum number of connections is reached for the real server, the FortiGate unit will automatically switch all further connection requests to another server until the connection number drops below the specified limit.</p> <p>0 means unlimited number of connections.</p> | 0 |

| Variable | Description | Default |
|---------------------------------------|--|-------------|
| monitor <healthcheck_str> | <p>Enter one or more names of health check monitor settings to use when performing a health check, separating each name with a space. If any of the configured health check monitors detect failures, the FortiGate unit will deem the server unresponsive, and will not forward traffic to that server. For details on configuring health check monitor settings, see “firewall ldb-monitor” on page 145.</p> <p>This option appears only if <code>healthcheck</code> is enable.</p> | No default. |
| port <port_ip> | Enter the port used if port forwarding is enabled. | 10 |
| status { active disable standby } | <p>Select whether the server is in the pool of servers currently being used for server load balanced traffic, the server is on standby, or is disabled.</p> <ul style="list-style-type: none"> <code>active</code>: The FortiGate unit may forward traffic to the server unless its health check monitors determine that the server is unresponsive, at which time the FortiGate unit will temporarily use a server whose <code>status</code> is <code>standby</code>. The <code>healthcheck</code> monitor will continue to monitor the unresponsive server for the duration of <code>holddown-interval</code>. If this server becomes reliably responsive again, it will be restored to active use, and the standby server will revert to standby. For details on health check monitoring when an active server is unresponsive, see “holddown-interval <seconds_int>” on page 239. <code>disable</code>: The FortiGate unit will not forward traffic to this server, and will not perform health checks. You might use this option to conserve server load balancing resources when you know that a server will be unavailable for a long period, such as when the server is down for repair. <code>standby</code>: If a server whose <code>status</code> is <code>active</code> becomes unresponsive, the FortiGate unit will temporarily use a responsive server whose <code>status</code> is <code>standby</code> until the server whose <code>status</code> is <code>active</code> again becomes reliably responsive. If multiple responsive standby servers are available, the FortiGate unit selects the standby server with the greatest <code>weight</code>. If a standby server becomes unresponsive, the FortiGate unit will select another responsive server whose <code>status</code> is <code>standby</code>. | active |
| weight <loadbalanceweight_int> | <p>Enter the weight value of a specific server. Servers with a greater weight receive a greater proportion of forwarded connections, or, if their <code>status</code> is <code>standby</code>, are more likely to be selected to temporarily replace servers whose <code>status</code> is <code>active</code>, but that are unresponsive. Valid weight values are between 1 and 255.</p> <p>This option is available only if <code>ldb-method</code> is <code>weighted</code>.</p> | 1 |

| Variable | Description | Default |
|---|---|--|
| ssl-cipher-suites The following are the variables for <code>config ssl-cipher-suites</code> , and are available only if <code>type</code> is <code>server-load-balance</code> and <code>ssl-algorithm</code> is <code>custom</code> . | | |
| <code>cipher <cipher_name></code> | Enter the cipher name. For a list of available ciphers, enter <code>set cipher ?</code> | |
| <code>versions {ssl-3.0 tls-1.0 tls-1.1}</code> | Enter the algorithm versions to support. | <code>ssl-3.0 tls-1.0 tls-1.1</code> |

vip46

Use this command to configure static NAT virtual IPv4 addresses for IPv6 addresses.

Syntax

```
config firewall vip46
  edit <name_str>
    set arp-reply {enable | disable}
    set color <color_int>
    set comment <comment_str>
    set extip <address_ipv4>[-address_ipv4]
    set extport <port_int>
    set id <id_num_str>
    set mappedip [<start_ipv6>-<end_ipv6>]
    set mappedport <port_int>
    set portforward {enable | disable}
    set src-filter <addr_str>
  end
```

| Variable | Description | Default |
|--|---|-------------|
| <name_str> | Enter the name of this virtual IP address. | No default. |
| arp-reply {enable disable} | Select to respond to ARP requests for this virtual IP address. | enable |
| color <color_int> | Enter the number of the color to use for the group icon in the web-based manager. | 0 |
| comment <comment_str> | Enter comments relevant to the configured virtual IP. | No default |
| extip <address_ipv4>[- address_ipv4] | <p>Enter the IP address or address range on the external interface that you want to map to an address or address range on the destination network.</p> <p>If mappedip is an IP address range, the FortiGate unit uses extip as the first IP address in the external IP address range, and calculates the last IP address required to create an equal number of external and mapped IP addresses for one-to-one mapping.</p> <p>To configure a dynamic virtual IP that accepts connections destined for any IP address, set extip to 0.0.0.0.</p> | 0.0.0.0 |
| extport <port_int> | <p>Enter the external port number that you want to map to a port number on the destination network.</p> <p>This option only appears if portforward is enabled.</p> <p>If portforward is enabled and you want to configure a static NAT virtual IP that maps a range of external port numbers to a range of destination port numbers, set extport to the first port number in the range. Then set mappedport to the start and end of the destination port range. The FortiGate unit automatically calculates the end of the extport port number range.</p> | 0 |

| Variable | Description | Default |
|---------------------------------------|--|-------------|
| id <id_num_str> | Enter a unique identification number for the configured virtual IP. Not checked for uniqueness. Range 0 - 65535. | No default. |
| mappedip [<start_ipv6>-<end_ipv6>] | <p>Enter the IP address or IP address range on the destination network to which the external IP address is mapped.</p> <p>If <code>mappedip</code> is an IP address range, the FortiGate unit uses <code>extip</code> as the first IP address in the external IP address range, and calculates the last IP address required to create an equal number of external and mapped IP addresses for one-to-one mapping.</p> <p>If <code>mappedip</code> is an IP address range, the FortiGate unit uses <code>extip</code> as a single IP address to create a one-to-many mapping.</p> | :: |
| mappedport <port_int> | <p>Enter the port number on the destination network to which the external port number is mapped.</p> <p>You can also enter a port number range to forward packets to multiple ports on the destination network.</p> <p>For a static NAT virtual IP, if you add a map to port range the FortiGate unit calculates the external port number range.</p> | 0 |
| portforward {enable disable} | Select to enable port forwarding. You must also specify the port forwarding mappings by configuring <code>extport</code> and <code>mappedport</code> . | disable |
| src-filter <addr_str> | Enter a source address filter. Each address must be in the form of an IPv4 subnet (x.x.x.x/n). Separate addresses with spaces. | null |

vip6

Use this command to configure static NAT virtual IPs for IPv6 addresses.

Syntax

```
config firewall vip6
  edit <name_str>
    set arp-reply {enable | disable}
    set color <color_int>
    set comment <comment_str>
    set extip <address_ipv6>[-address_ipv6]
    set extport <port_int>
    set id <id_num_str>
    set mappedip [<start_ipv6>-<end_ipv6>]
    set mappedport <port_int>
    set portforward {enable | disable}
    set protocol {sctp | tcp | udp}
    set src-filter <addr_str>
    set type static-nat
  end
```

| Variable | Description | Default |
|--|--|-------------|
| <name_str> | Enter the name of this virtual IP address. | No default. |
| arp-reply {enable disable} | Select to respond to ARP requests for this virtual IP address. | enable |
| color <color_int> | Enter the number of the color to use for the group icon in the web-based manager. | 0 |
| comment <comment_str> | Enter comments relevant to the configured virtual IP. | No default |
| extip <address_ipv6>[- address_ipv6] | <p>Enter the IP address or address range on the external interface that you want to map to an address or address range on the destination network.</p> <p>If mappedip is an IP address range, the FortiGate unit uses extip as the first IP address in the external IP address range, and calculates the last IP address required to create an equal number of external and mapped IP addresses for one-to-one mapping.</p> <p>To configure a dynamic virtual IP that accepts connections destined for any IP address, set extip to 0.0.0.0.</p> | 0.0.0.0 |

| Variable | Description | Default |
|---------------------------------------|--|-------------|
| extport <port_int> | <p>Enter the external port number that you want to map to a port number on the destination network.</p> <p>This option only appears if <code>portforward</code> is enabled.</p> <p>If <code>portforward</code> is enabled and you want to configure a static NAT virtual IP that maps a range of external port numbers to a range of destination port numbers, set <code>extport</code> to the first port number in the range. Then set <code>mappedport</code> to the start and end of the destination port range. The FortiGate unit automatically calculates the end of the <code>extport</code> port number range.</p> | 0 |
| id <id_num_str> | Enter a unique identification number for the configured virtual IP. Not checked for uniqueness. Range 0 - 65535. | No default. |
| mappedip [<start_ipv6>-<end_ipv6>] | <p>Enter the IP address or IP address range on the destination network to which the external IP address is mapped.</p> <p>If <code>mappedip</code> is an IP address range, the FortiGate unit uses <code>extip</code> as the first IP address in the external IP address range, and calculates the last IP address required to create an equal number of external and mapped IP addresses for one-to-one mapping.</p> | 0.0.0.0 |
| mappedport <port_int> | <p>Enter the port number on the destination network to which the external port number is mapped.</p> <p>You can also enter a port number range to forward packets to multiple ports on the destination network.</p> <p>For a static NAT virtual IP, if you add a map to port range the FortiGate unit calculates the external port number range.</p> | 0 |
| portforward {enable disable} | Select to enable port forwarding. You must also specify the port forwarding mappings by configuring <code>extport</code> and <code>mappedport</code> . | disable |
| protocol {sctp tcp udp} | Select the protocol, TCP or UDP, to use when forwarding packets. | tcp |
| src-filter <addr_str> | Enter a source address filter. Each address must be in the form of an IPv6 subnet (x:x:x:x:x:x/n). Separate addresses with spaces. | null |
| type static-nat | Only static NAT VIP is available in IPv6. | static-nat |

vip64

Use this command to configure static NAT virtual IPv6 addresses for IPv4 addresses.

Syntax

```
config firewall vip64
  edit <zname_str>
    set arp-reply {enable | disable}
    set color <color_int>
    set comment <comment_str>
    set extip <address_ipv6>[-address_ipv6]
    set extport <port_int>
    set id <id_num_str>
    set mappedip [<start_ipv4>-<end_ipv4>]
    set mappedport <port_int>
    set portforward {enable | disable}
    set src-filter <addr_str>
  end
```

| Variable | Description | Default |
|--|--|-------------|
| <zname_str> | Enter the name of this virtual IP address. | No default. |
| arp-reply {enable disable} | Select to respond to ARP requests for this virtual IP address. | enable |
| color <color_int> | Enter the number of the color to use for the group icon in the web-based manager. | 0 |
| comment <comment_str> | Enter comments relevant to the configured virtual IP. | No default |
| extip <address_ipv6>[- address_ipv6] | Enter the IP address or address range on the external interface that you want to map to an address or address range on the destination network. If mappedip is an IP address range, the FortiGate unit uses extip as the first IP address in the external IP address range, and calculates the last IP address required to create an equal number of external and mapped IP addresses for one-to-one mapping. To configure a dynamic virtual IP that accepts connections destined for any IP address, set extip to ::. | :: |
| extport <port_int> | Enter the external port number that you want to map to a port number on the destination network. This option only appears if portforward is enabled. If portforward is enabled and you want to configure a static NAT virtual IP that maps a range of external port numbers to a range of destination port numbers, set extport to the first port number in the range. Then set mappedport to the start and end of the destination port range. The FortiGate unit automatically calculates the end of the extport port number range. | 0 |
| id <id_num_str> | Enter a unique identification number for the configured virtual IP. Not checked for uniqueness. Range 0 - 65535. | No default. |

| Variable | Description | Default |
|---------------------------------------|--|---------|
| mappedip [<start_ipv4>-<end_ipv4>] | <p>Enter the IP address or IP address range on the destination network to which the external IP address is mapped.</p> <p>If mappedip is an IP address range, the FortiGate unit uses extip as the first IP address in the external IP address range, and calculates the last IP address required to create an equal number of external and mapped IP addresses for one-to-one mapping.</p> <p>If mappedip is an IP address range, the FortiGate unit uses extip as a single IP address to create a one-to-many mapping.</p> | 0.0.0.0 |
| mappedport <port_int> | <p>Enter the port number on the destination network to which the external port number is mapped.</p> <p>You can also enter a port number range to forward packets to multiple ports on the destination network.</p> <p>For a static NAT virtual IP, if you add a map to port range the FortiGate unit calculates the external port number range.</p> | 0 |
| portforward {enable disable} | Select to enable port forwarding. You must also specify the port forwarding mappings by configuring extport and mappedport. | disable |
| src-filter <addr_str> | Enter a source address filter. Each address must be in the form of an IPv4 subnet (x:x:x:x:x:x/n). Separate addresses with spaces. | null |

vipgrp

You can create virtual IP groups to facilitate firewall policy traffic control. For example, on the DMZ interface, if you have two email servers that use Virtual IP mapping, you can put these two VIPs into one VIP group and create one external-to-DMZ policy, instead of two policies, to control the traffic.

Firewall policies using VIP Groups are matched by comparing both the member VIP IP address(es) and port number(s).

Syntax

```
config firewall vipgrp
  edit <name_str>
    set interface <name_str>
    set member <virtualip_str>
  end
```

| Variable | Description | Default |
|---------------------------|--|-------------|
| <name_str> | Enter the name of the virtual IP group. | No default. |
| interface <name_str> | Enter the name of the interface to which the virtual IP group will be bound. | No default. |
| member <virtualip_str> | Enter one or more virtual IPs that will comprise the virtual IP group. | No default. |

vipgrp46

Use this command to create a vip46 virtual IP group.

Syntax

```
config firewall vipgrp46
  edit <name_str>
    set color <color_int>
    set comments <str>
    set member <virtualip_str>
  end
```

| Variable | Description | Default |
|------------------------|---|-------------|
| <name_str> | Enter the name of the virtual IP group. | No default. |
| color <color_int> | Enter the number of the color to use for the group icon in the web-based manager. | 0 |
| comments <str> | Optionally, enter a comment. | No default. |
| member <virtualip_str> | Enter one or more vip46 virtual IPs that will comprise the virtual IP group. | No default. |

vipgrp64

Use this command to create a vip64 virtual IP group.

Syntax

```
config firewall vipgrp46
  edit <name_str>
    set color <color_int>
    set comments <str>
    set member <virtualip_str>
  end
```

| Variable | Description | Default |
|------------------------|---|-------------|
| <name_str> | Enter the name of the virtual IP group. | No default. |
| color <color_int> | Enter the number of the color to use for the group icon in the web-based manager. | 0 |
| comments <str> | Optionally, enter a comment. | No default. |
| member <virtualip_str> | Enter one or more vip64 virtual IPs that will comprise the virtual IP group. | No default. |

ftp-proxy

Use ftp-proxy commands to configure the FortiGate explicit FTP proxy. You can use the FortiGate explicit FTP proxy and interface settings to enable explicit FTP proxying on one or more interfaces. When enabled, the FortiGate unit becomes a FTP proxy server. All FTP sessions received by interfaces with explicit FTP proxy enabled are intercepted by the explicit FTP proxy relayed to their destinations.

To use the explicit FTP proxy, users must add the IP address of a FortiGate interface and the explicit proxy port number to the proxy configuration settings of their FTP clients.

[explicit](#)

explicit

Use this command to enable the explicit FTP proxy, and configure the TCP port used by the explicit FTP proxy.

Syntax

```
config ftp-proxy explicit
  set status {disable | enable}
  set incoming-port <in_port_int>
  set incoming-ip <incoming_address_ipv4>
  set outgoing-ip <outgoing_address_ipv4>
  set sec-default-action {accept | deny}
end
```

| Variable | Description | Default |
|--|--|---------|
| status {disable enable} | Enable the explicit FTP proxy for FTP sessions. | disable |
| incoming-port <in_port_int> | Enter the port number that traffic from FTP clients use to connect to the explicit FTP proxy. The range is 0 to 65535. Explicit FTP proxy users must configure their FTP client proxy settings to use this port. | 21 |
| incoming-ip <incoming_address_ipv4> | Enter the IP address of a FortiGate unit interface that should accept sessions for the explicit FTP proxy. Use this command to restrict the explicit FTP proxy to only accepting sessions from one FortiGate interface. The destination IP address of explicit FTP proxy sessions should match this IP address. This field is visible in NAT/Route mode only. | 0.0.0.0 |
| outgoing-ip <outgoing_address_ipv4> | Enter the IP address of a FortiGate unit interface that explicit FTP proxy sessions should exit the FortiGate unit from. Use this command to restrict the explicit FTP proxy to only allowing sessions to exit from one FortiGate interface. This IP address becomes the source address of FTP proxy sessions exiting the FortiGate unit. This field is visible in NAT/Route mode only. | |
| sec-default-action {accept deny} | Configure the explicit FTP proxy to block (deny) or accept sessions if firewall policies have not been added for the explicit FTP proxy. To add firewall policies for the explicit FTP proxy add a firewall policy and set the source interface to ftp-proxy. The default setting denies access to the explicit FTP proxy before adding a firewall policy. If you set this option to <code>accept</code> the explicit FTP proxy server accepts sessions even if you haven't added an ftp-proxy firewall policy. | deny |

gui

This chapter contains the following section:

[console](#)

console

This command stores a base-64 encoded file that contains configuration of the dashboard and *System > Status* web-based manager pages. This command is not user configurable

Syntax

```
config gui console
    set preferences <filedata>
end
```

| Variable | Description | Default |
|------------------------|---|-------------|
| preferences <filedata> | Base-64 encoded file to upload containing the commands to set up the web-based manager CLI console on the FortiGate unit. | No default. |

icap

This chapter contains the following sections:

[profile](#)

[server](#)

profile

Use this command to configure an Internet Content Adaptation Protocol (ICAP) profile.

Syntax

```
config icap profile
  edit <icap_profile_name>
    set replacemsg-group <grp_name>
    set request {enable | disable}
    set response {enable | disable}
    set streaming-content-bypass {enable | disable}
  end
```

| Variable | Description | Default |
|---|---|---------|
| <icap_profile_name> | Enter the ICAP profile name. | |
| replacemsg-group <grp_name> | Enter the replacement message group name. | |
| request {enable disable} | Enable to send requests to an ICAP server. | disable |
| response {enable disable} | Enable to send HTTP responses to an ICAP server. | disable |
| streaming-content-bypass {enable disable} | Enable to bypass the ICAP server for streaming content. | disable |

server

Use this command to configure Internet Content Adaptation Protocol (ICAP) servers.

Syntax

```
config icap server
  edit <icap_server_name>
    set ip-version {4 | 6}
    set ip-address <server_ipv4>
    set ip6-address <server_ipv6>
    set max-connections <int>
    set port <port_int>
  end
```

| Variable | Description | Default |
|---------------------------|---|---------|
| <icap_server_name> | Enter the ICAP profile name. | |
| ip-version {4 6} | Select IPv4 or IPv6 addressing. | 4 |
| ip-address <server_ipv4> | Enter the ICAP server IP address (IPv4). | 0.0.0.0 |
| ip6-address <server_ipv6> | Enter the ICAP server IP address (IPv6). | :: |
| max-connections <int> | Enter the maximum permitted number of concurrent connections to the ICAP server. Range: 1-65 535. | 100 |
| port <port_int> | Enter the ICAP server port number. | 1344 |

imp2p

Use imp2p commands to configure user access to Instant Messaging and Peer-to-Peer applications, and to configure a global policy for unknown users who might use these applications.

This chapter contains the following sections:

[aim-user](#)

[icq-user](#)

[msn-user](#)

[old-version](#)

[policy](#)

[yahoo-user](#)

aim-user

Use this command to permit or deny a specific user the use of AOL Instant Messenger.

Syntax

```
config imp2p aim-user
  edit <name_str>
    set action {deny | permit}
  end
```

| Variable | Description | Default |
|------------------------|---|---------|
| name_str | The name of the AIM user. | |
| action {deny permit} | Permit or deny the use of AOL Instant Messenger by this user. | deny |

icq-user

Use this command to permit or deny a specific user the use of ICQ Instant Messenger.

Syntax

```
config imp2p icq-user
  edit <name_str>
    set action {deny | permit}
  end
```

| Variable | Description | Default |
|------------------------|---|---------|
| name_str | The name of the ICQ user. | |
| action {deny permit} | Permit or deny the use of the ICQ Instant Messenger by this user. | deny |

msn-user

Use this command to permit or deny a specific user the use of MSN Messenger.

Syntax

```
config imp2p msn-user
  edit <name_str>
    set action {deny | permit}
  end
```

| Variable | Description | Default |
|------------------------|---|---------|
| name_str | The name of the MSN user. | |
| action {deny permit} | Permit or deny the use of MSN Messenger by this user. | deny |

old-version

Some older versions of IM protocols are able to bypass file blocking because the message types are not recognized. The following command provides the option to disable these older IM protocol versions. Supported IM protocols include:

- MSN 6.0 and above
- ICQ 4.0 and above
- AIM 5.0 and above
- Yahoo 6.0 and above

Syntax

```
config imp2p old-version
    set aim {best-effort | block}
    set icq {best-effort | block}
    set msn {best-effort | block}
    set yahoo {best-effort | block}
end
```

| Variable | Description | Default |
|-----------------------------|--|---------|
| aim {best-effort block} | Enter <code>block</code> to block the session if the version is too old. Enter <code>best-effort</code> to inspect the session based on the policy. | block |
| icq {best-effort block} | Enter <code>block</code> to block the session if the version is too old. Enter <code>best-effort</code> to inspect the session based on the policy. | block |
| msn {best-effort block} | Enter <code>block</code> to block the session if the version is too old. Enter <code>best-effort</code> to inspect the session based on the policy. | block |
| yahoo {best-effort block} | Enter <code>block</code> to block the session if the version is too old. Enter <code>best-effort</code> to inspect the session based on the policy. | block |

policy

Use this command to create a global policy for instant messenger applications. If an unknown user attempts to use one of the applications, the user can either be permitted use and added to a white list, or be denied use and added to a black list.



The imp2p settings are part of Application Control. When creating a new VDOM, the default imp2p policy settings are set to `allow`, thereby permitting the settings in Application Control to drive the configuration.

Syntax

```
config imp2p policy
  set aim {allow | deny}
  set icq {allow | deny}
  set msn {allow | deny}
  set yahoo {allow | deny}
end
```

| Variable | Description | Default |
|----------------------|---|---------|
| aim {allow deny} | Allow an unknown user and add the user to the white list. Deny an unknown user and add the user to the black list. | allow |
| icq {allow deny} | Allow an unknown user and add the user to the white list. Deny an unknown user and add the user to the black list. | allow |
| msn {allow deny} | Allow an unknown user and add the user to the white list. Deny an unknown user and add the user to the black list. | allow |
| yahoo {allow deny} | Allow an unknown user and add the user to the white list. Deny an unknown user and add the user to the black list. | allow |

yahoo-user

Use this command to permit or deny a specific user the use of Yahoo Messenger.

Syntax

```
config imp2p yahoo-user
  edit <name_str>
    set action {deny | permit}
  end
```

| Variable | Description | Default |
|------------------------|---|---------|
| name_str | The name of the Yahoo user. | |
| action {deny permit} | Permit or deny the use of Yahoo Messenger by this user. | deny |

ips

Use ips commands to configure IPS sensors to define which signatures are used to examine traffic and what actions are taken when matches are discovered. DoS sensors can also be defined to examine traffic for anomalies

This chapter contains the following sections:

[custom](#)

[decoder](#)

[global](#)

[rule](#)

[sensor](#)

[setting](#)



If the IPS test can't find the destination MAC address, the peer interface will be used. To ensure packets get IPS inspection, there must be a Peer Interface. Both interfaces must be in the same VDOM, and one interface cannot be both the peer and original interface. For information on how to set the Peer Interface see ["interface" on page 555](#).

custom

Create custom IPS signatures and add them to IPS sensors.

Custom signatures provide the power and flexibility to customize FortiGate Intrusion Protection for diverse network environments. The FortiGate predefined signatures cover common attacks. If an unusual or specialized application or an uncommon platform is being used, add custom signatures based on the security alerts released by the application and platform vendors.

Use custom signatures to block or allow specific traffic.

The custom signature settings are configured when it is defined as a signature override in an IPS sensor. This way, a single custom signature can be used in multiple sensors with different settings in each.



Custom signatures are an advanced feature. This document assumes the user has previous experience writing intrusion detection signatures.

Syntax

```
config ips custom
  edit <sig_str>
    set signature <signature_str>
  end
```

| Variable | Description | Default |
|---------------------------|--|-------------|
| sig_str | The name of the custom signature. | |
| signature <signature_str> | Enter the custom signature. The signature must be enclosed in single quotes. | No default. |

decoder

The Intrusion Protection system looks for certain types of traffic on specific ports. Using the decoders command, you can change ports if your configuration uses non-standard ports.

Syntax

```
config ips decoder <decoder_str>
    set port_list <port_int>
end
```

| Variable | Description | Default |
|----------------------|--|-------------------|
| <decoder_str> | Enter the name of the decoder. Enter '?' for a list. | |
| port_list <port_int> | Enter the ports which the decoder will examine. Multiple ports can be specified by separating them with commas and enclosing the list in quotes. | varies by decoder |

global

Use this command to set IPS operating parameters.

Syntax

```
config ips global
  set algorithm {engine-pick | low | high | super}
  set anomaly-mode {continuous | periodical}
  set database {regular | extended}
  set engine-count <integer>
  set fail-open {enable | disable}
  set hardware-accel-mode {engine-pick | cp-only | np-only | np-cp
    | none}
  set session-limit-mode {accurate | heuristic}
  set skype-client-public-ipaddr <IP_addr_list>
  set socket-size <ips_buffer_size>
  set traffic-submit {enable | disable}
end
```

| Variable | Description | Default |
|--|---|-------------|
| algorithm {engine-pick low high super} | The IPS engine has two methods to determine whether traffic matches signatures. <ul style="list-style-type: none"> low is a slower method that uses less memory high is a faster method that uses more memory super is a method that works well on models with more than 4GB memory engine-pick allows the IPS engine to choose the best method on the fly. | engine-pick |
| anomaly-mode {continuous periodical} | Enter continuous to start blocking packets once attack starts. Enter periodical to allow configured number of packets per second. | continuous |
| database {regular extended} | Select regular or extended IPS database. | regular |
| engine-count <integer> | Enter the number of intrusion protection engines to run. Multi-processor FortiGate units can more efficiently process traffic with multiple engines running. When set to the default value of 0, the FortiGate unit determines the optimal number of intrusion protection engines. | 0 |
| fail-open {enable disable} | If for any reason the IPS should cease to function, it will fail open by default. This means that crucial network traffic will not be blocked and the Firewall will continue to operate while the problem is resolved. | enable |
| hardware-accel-mode {engine-pick cp-only np-only np-cp none} | Set hardware acceleration mode. CP refers to Content Processor, NP to Network Processor. none disables hardware acceleration. engine-pick automatically chooses the best acceleration level. | engine-pick |
| session-limit-mode {accurate heuristic} | Enter accurate to accurately count the concurrent sessions. This option demands more resources. Enter heuristic to heuristically count the concurrent sessions. | heuristic |

| Variable | Description | Default |
|---|--|-----------------|
| skype-client-public-ipaddr <IP_addr_list> | Enter the public IP addresses of your network that are used for Skype sessions. This will help the FortiGate unit identify Skype sessions properly in the Sessions dashboard widget. Separate IP addresses with commas, not spaces. | No default. |
| socket-size <ips_buffer_size> | Set intrusion protection buffer size. The default value is correct in most cases. | model-dependent |
| traffic-submit {enable disable} | Submit attack characteristics to FortiGuard Service | disable |

rule

The IPS sensors use signatures to detect attacks. These signatures can be listed with the rules command. Details about the default settings of each signature can also be displayed.

Syntax

```
config ips rule <rule_str>
get
```

| Variable | Description | Default |
|------------|---|---------|
| <rule_str> | Enter the name of a signature. For a complete list of the predefined signatures, enter '?' instead of a signature name. | |

Example

This example shows how to display the current configuration of the Apache.Long.Header.DoS signature.

```
# config ips rule Apache.Long.Header.DoS
(Apache.Long.He~d) # get
name                : Apache.Long.Header.DoS
status              : enable
log                 : enable
log-packet          : disable
action              : pass
group               : web_server
severity            : medium
location            : server
os                  : Windows, Linux, BSD, Solaris
application         : Apache
service             : TCP, HTTP
rule-id             : 11206
rev                 : 2.335
```

sensor

The IPS sensors use signatures to detect attacks. IPS sensors are made up of filters and override rules. Each filter specifies a number of signature attributes and all signatures matching all the specified attributes are included in the filter. Override rules allow you to override the settings of individual signatures.

Syntax

```
config ips sensor
  edit <sensor_str>
    get
    set comment <comment_str>
    set log {disable | enable}
    config entries
      edit <filter_int>
        set location {all | client | server}
        set severity {all | info low medium high critical}
        set protocol <protocol_str>
        set os {all | other windows linux bsd solaris macos}
        set application <app_str>
        set status {default | enable | disable}
        set tags <tags_str>
        set log {default | enable | disable}
        set log-packet {disable | enable}
        set action {block | default | pass | reject}
        set quarantine {attacker | both | interface | none}
        set quarantine-expiry <minutes_int>
        set quarantine-log {disable | enable}
        set rate-count <count_int>
        set rate-duration <seconds_int>
        set rate-mode <continuous | periodical>
        set rate-track <dest-ip | dhcp-client-mac | dns-domain
          | none | src-ip>
        set rule [<rule1_int> <rule2_int> ... ]
      get
      config exempt-ip
        edit <exempt-ip_id>
          set dst-ip <ip4mask>
          set src-ip <ip4mask>
        end
      end
    end
  end
```

| Variable | Description | Default |
|--|---|---------|
| <sensor_str> | Enter the name of an IPS sensor. For a list of the IPS sensors, enter '?' instead of an IPS sensor name. Enter a new name to create a sensor. | |
| comment <comment_str> | Enter a description of the IPS sensor. This description will appear in the ISP sensor list. Descriptions with spaces must be enclosed in quotes. | |
| log {disable enable} | Enable or disable IPS logging. | enable |
| <filter_int> | Enter the ID number of a filter. For a list of the IDs in the IPS sensor, enter '?' instead of an ID. Enter a new ID to create a filter. | |
| location {all client server} | Specify the type of system to be protected. <ul style="list-style-type: none"> client selects signatures for attacks against client computers. server selects signatures for attacks against servers. all selects both client and server signatures. | all |
| severity {all info low medium high critical} | Specify the severity level or levels. Specify all to include all severity levels. | all |
| protocol <protocol_str> | Specify the protocols to be examined. Enter '?' to display a list of the available protocols. All will include all protocols. Other will include all unlisted protocols. | all |
| os {all other windows linux bsd solaris macos} | Specify the operating systems to be protected. All will include all operating systems. Other will include all unlisted operating systems. | all |
| application <app_str> | Specify the applications to be protected. Enter '?' to display a list of the available applications. All will include all applications. Other will include all unlisted applications. | all |
| status {default enable disable} | Specify the status of the signatures included in the filter. <ul style="list-style-type: none"> enable will enable the filter. disable will disable the filter. default will enable the filter and only use the filters with a default status of enable. Filters with a default status of disable will not be used. | default |
| tags <tags_str> | Enter object tags applied to this filter. Separate tag names with spaces. | null |
| log {default enable disable} | Specify the logging status of the signatures included in the filter. <ul style="list-style-type: none"> enable will enable logging. disable will disable logging. default will enable logging for only the filters with a default logging status of enable. Filters with a default logging status of disable will not be logged. | default |

| Variable | Description | Default |
|---|--|------------|
| log-packet {disable enable} | When enabled, packet logging will save the packet that triggers the filter. You can download the packets in pcap format for diagnostic use. This feature is only available in FortiGate units with internal hard drives. | disable |
| action {block default pass reject} | Specify what action is taken with traffic in which signatures are detected. <ul style="list-style-type: none"> block will drop the session with the offending traffic. pass will allow the traffic. reject will reset the session. default will either pass or drop matching traffic, depending on the default action of each signature. | default |
| quarantine {attacker both interface none} | To prevent the attacker from continuing to attack the FortiGate unit, you can quarantine the attacker to the banned user list in one of three ways. <ul style="list-style-type: none"> Enter <code>attacker</code> to block all traffic sent from the attacker's IP address. The attacker's IP address is also added to the banned user list. The target's address is not affected. Enter <code>both</code> to block all traffic sent from the attacker's IP address to the target (victim's) IP address. Traffic from the attacker's IP address to addresses other than the victim's IP address is allowed. The attacker's and target's IP addresses are added to the banned user list as one entry. Enter <code>interface</code> to block all traffic from connecting to the FortiGate unit interface that received the attack. The interface is added to the banned user list. Enter <code>none</code> to disable the adding of addresses to the quarantine but the current DoS sensor. | none |
| quarantine-expiry <minutes_int> | Enter the duration of the quarantine in minutes. Range 0 to 259200. | 5 |
| quarantine-log {disable enable} | Enable or disable writing a log message when a user is quarantined. | |
| rate-count <count_int> | Set the threshold (number of signature matches) that triggers the sensor. Range 1 to 65 535. 0 disables. | 0 |
| rate-duration <seconds_int> | Set the duration over which the rate-count is measured. Use rate-mode to determine how the duration is applied. Range 1 to 65 535. | 60 |
| rate-mode <continuous periodical> | Select how rate-count is applied: <ul style="list-style-type: none"> continuous — action is applied as soon as rate-count is reached periodical — action is applied when rate-count is reached during rate-duration period | continuous |
| rate-track <dest-ip dhcp-client-mac dns-domain none src-ip> | Select which protocol field within the packet to track. | none |

| Variable | Description | Default |
|--|--|---------|
| rule [<rule1_int> <rule2_int> ...] | To add predefined or custom IPS signatures, specify the rule IDs of the signatures. | null |
| get fields | | |
| get - when used in edit <sensor_str> | <p>This get command returns the following information about the sensor:</p> <ul style="list-style-type: none"> • <code>name</code> is the name of this sensor. • <code>comment</code> is the comment entered for this sensor. • <code>count-enabled</code> is the number of enabled signatures in this IPS sensor. Disabled signatures are not included. • <code>count-pass</code> is the number of enabled signatures configured with the <code>pass</code> action. • <code>count-block</code> is the number of enabled signatures configured with the <code>block</code> action. • <code>count-reset</code> is the number of enabled signatures configured with the <code>reset</code> action. • <code>filter</code> lists the filters in this IPS sensor. • <code>override</code> lists the overrides in the IPS sensor. | |
| get - when used in edit <filter_int> | <p>This get command returns the following information about the filter:</p> <ul style="list-style-type: none"> • <code>name</code> is the name of this filter. • <code>count</code> is the total number of signatures in this filter. Both enabled and disabled signatures are included. • <code>location</code> is type of system targeted by the attack. The locations are client and server. • <code>severity</code> is the relative importance of the signature, from info to critical. • <code>protocol</code> is the type of traffic to which the signature applies. Examples include HTTP, POP3, H323, and DNS. • <code>os</code> is the operating systems to which the signature applies. • <code>application</code> is the program affected by the signature. • <code>status</code> displays whether the signature state is enabled, disabled, or default. • <code>log</code> displays the logging status of the signatures included in the filter. Logging can be set to enabled, disabled, or default. • <code>action</code> displays what the FortiGate does with traffic containing a signature. The action can be set to pass all, block all, reset all, or default. • <code>quarantine</code> displays how the FortiGate unit will quarantine attackers. | |

| Variable | Description | Default |
|--|---|-----------------|
| config exempt-ip fields | | |
| This subcommand is available after <code>rule</code> has been set. | | |
| edit <exempt-ip_id> | Enter the ID number of an exempt-ip entry. For a list of the exempt-ip entries in the IPS sensor, enter '?' instead of an ID. Enter a new ID to create a new exempt-ip. | |
| dst-ip <ip4mask> | Enter the destination IP address and netmask to exempt. | 0.0.0.0 0.0.0.0 |
| src-ip <ip4mask> | Enter the source IP address and netmask to exempt. | 0.0.0.0 0.0.0.0 |

setting

Use the IPS settings command to configure settings for IPS packet logging.

Syntax

```
config ips settings
  set ips-packet-quota <MB_int>
  set packet-log-history <packets_int>
  set packet-log-memory <KB_int>
  set packet-log-post-attack <packets_int>
end
```

| Variable | Description | Default |
|---|---|---------|
| ips-packet-quota <MB_int> | Enter the maximum amount of disk space to use for logged packets when logging to disk. The acceptable range is from 0 to 4294967295 megabytes. This command affects only logging to disk. | 0 |
| packet-log-history <packets_int> | <p>Enter the number of packets to capture before and including the one in which the IPS signature is detected.</p> <p>If the value is more than 1, the packet containing the signature is saved in the packet log, as well as those preceding it, with the total number of logged packets equalling the packet-log-history setting. For example, if packet-log-history is set to 7, the FortiGate unit will save the packet containing the IPS signature match and the six before it.</p> <p>The acceptable range for packet-log-history is from 1 to 255. The default is 1.</p> <p>Setting packet-log-history to a value larger than 1 can affect the performance of the FortiGate unit because network traffic must be buffered. The performance penalty depends on the model, the setting, and the traffic load.</p> | 1 |
| packet-log-memory <KB_int> | Enter the maximum amount of memory to use for logged packets when logging to memory. The acceptable range is from 64 to 8192 kilobytes. This command affects only logging to memory. | 256 |
| packet-log-post-attack <packets_int> | <p>Enter how many packets are logged after the one in which the IPS signature is detected. For example, if packet-log-post-attack is set to 10, the FortiGate unit will save the ten packets following the one containing the IPS signature match.</p> <p>The acceptable range for packet-log-post-attack is from 0 to 255. The default is 0.</p> | 0 |

log

Use the `config log` commands to set the logging type, the logging severity level, and the logging location for the FortiGate unit.



In Transparent mode, certain log settings and options may not be available because certain features do not support logging or are not available in this mode. For example, SSL VPN events are not available in Transparent mode.

[custom-field](#)

[{disk | fortianalyzer | fortianalyzer2 | fortianalyzer3 | memory | syslogd | syslogd2 | syslogd3 | webtrends | fortiguard} filter](#)

[disk setting](#)

[eventfilter](#)

[{fortianalyzer | syslogd} override-filter](#)

[fortianalyzer override-setting](#)

[{fortianalyzer | fortianalyzer2 | fortianalyzer3} setting](#)

[fortiguard setting](#)

[gui-display](#)

[memory setting](#)

[memory global-setting](#)

[setting](#)

[syslogd override-setting](#)

[{syslogd | syslogd2 | syslogd3} setting](#)

[webtrends setting](#)

custom-field

Use the following command to customize the log fields with a name and/or value. The custom name and/or value will appear in the log message.

Syntax

```
config log custom-field
  edit id <integer>
    set name <name>
    set value <integer>
  end
```

| Variable | Description | Default |
|-----------------|---|------------|
| id <integer> | Enter the identification number for the log field. | No default |
| name <name> | Enter a name to identify the log. You can use letters, numbers, ('_'), but no characters such as the number symbol (#). The name cannot exceed 16 characters. | No default |
| value <integer> | Enter a firewall policy number to associate a firewall policy with the logs. | No default |

{disk | fortianalyzer | fortianalyzer2 | fortianalyzer3 | memory | syslogd | syslogd2 | syslogd3 | webtrends | fortiguard} filter

Use this command to configure log filter options. Log filters define the types of log messages sent to each log location. Use the ? command to view each filter setting since not all filter settings display for each device.

Filter settings for fortiguard are only available when FortiGuard Analysis and Management Service is enabled. Filter settings for disk is available only for FortiGate units with hard disks.

Syntax

```
config log {disk | fortianalyzer | fortianalyzer2 | fortianalyzer3
    |memory | syslogd | syslogd2 | syslogd3 | webtrends |
    fortiguard} filter
    set analytics {enable | disable}
    set anomaly {enable | disable}
    set app-crt1 {enable | disable}
    set app-crt1-all {enable | disable}
    set attack {enable | disable}
    set blocked {enable | disable}
    set discovery {enable | disable}
    set dlp {enable | disable}
    set dlp-all {enable | disable}
    set dlp-archive {enable | disable}
    set dlp-docsource {enable | disable}
    set email {enable | disable}
    set email-log-google {enable | disable}
    set email-log-imap {enable | disable}
    set email-log-msn {enable | disable}
    set email-log-pop3 {enable | disable}
    set email-log-smtp {enable | disable}
    set email-log-yahoo {enable | disable}
    set forward-traffic {enable | disable}
    set ftgd-wf-block {enable | disable}
    set ftgd-wf-errors {enable | disable}
    set local-traffic {enable | disable}
    set gtp {enable | disable}
    set infected {enable | disable}
    set mass-mms {enable | disable}
    set multicast-traffic {enable | disable}
    set netscan {enable | disable}
    set oversized {enable | disable}
    set scanerror {enable | disable}
    set severity {alert | critical | debug | emergency | error |
        information | notification | warning}
    set signature {enable | disable}
    set suspicious {enable | disable}
    set switching-protocols {enable | disable}
    set traffic {enable | disable}
    set url-filter {enable | disable}
```

```

set virus {enable | disable}
set voip {enable | disable}
set vulnerability {enable | disable}
set web {enable | disable}
set web-content {enable | disable}
set web-filter-activex {enable | disable}
set web-filter-applet {enable | disable}
set web-filter-command-block {enable | disable}
set web-filter-cookie {enable | disable}
set web-filter-ftgd-quota {enable | disable}
set web-filter-ftgd-quota-counting {enable | disable}
set web-filter-ftgd-quota-expired {enable | disable}
set web-filter-script-other {enable | disable}
end

```

| Variable | Description | Default |
|--|--|---------|
| analytics {enable disable} | Enable or disable logging of FortiGuard Analytics messages. | enable |
| anomaly {enable disable} | Enable or disable logging all detected and prevented attacks based on unknown or suspicious traffic patterns, and the action taken by the FortiGate unit in the attack log. This field is available when <code>attack</code> is enabled. | enable |
| app-ctrl {enable disable} | Enable or disable logging of application control logs. | enable |
| app-ctrl-all {enable disable} | Enable or disable logging of the sub-category of application control logs. | disable |
| attack {enable disable} | Enable or disable the attack log. | enable |
| blocked {enable disable} | Enable or disable logging all instances of blocked files. | enable |
| discovery {enable disable} | Enable or disable logging of netscan discovery events. | enable |
| dlp {enable disable} | Enable or disable logging of data leak prevention events. | enable |
| dlp-all {enable disable} | Enable or disable logging of all data leak prevention subcategories. | disable |
| dlp-archive {enable disable} | Enable or disable logging of data leak prevention content archive events. | enable |
| dlp-docsource {enable disable} | Enable or disable logging of data leak prevention document source scanning events. | enable |
| email {enable disable} | Enable or disable the spam filter log. | enable |
| email-log-google {enable disable} | Enable or disable logging of spam detected in Gmail messages. | enable |
| email-log-imap {enable disable} | Enable or disable logging of spam detected in IMAP traffic. <code>email enable</code> only. | enable |
| email-log-msn {enable disable} | Enable or disable logging of spam detected in MSN email messages. | enable |
| email-log-pop3 {enable disable} | Enable or disable logging of spam detected in POP3 traffic. <code>email enable</code> only. | enable |

| Variable | Description | Default |
|--|--|-------------|
| email-log-smtp {enable disable} | Enable or disable logging of spam detected in SMTP traffic. email enable only. | enable |
| email-log-yahoo {enable disable} | Enable or disable logging of spam detected in Yahoo email messages. | enable |
| forward-traffic {enable disable} | Enable or disable logging of forwarded traffic messages. | enable |
| ftgd-wf-block {enable disable} | Enable or disable logging of web pages blocked by FortiGuard category filtering in the web filter log. This field is available when web is enabled. | enable |
| ftgd-wf-errors {enable disable} | Enable or disable logging all instances of FortiGuard category filtering rating errors. This field is available when web is enabled. | enable |
| local-traffic {enable disable} | Enable or disable logging of local-in or local-out traffic messages. | enable |
| gtp {enable disable} | Enable or disable FortiOS Carrier logging for GTP messages. | enable |
| infected {enable disable} | Enable or disable logging of all virus infections in the antivirus log. This field is available when virus is enabled. | enable |
| mass-mms {enable disable} | Enable or disable FortiOS Carrier logging of a large amount of MMS blocked messages. | enable |
| multicast-traffic {enable disable} | Enable or disable logging of multicast traffic messages. | enable |
| netscan {enable disable} | Enable or disable logging of network vulnerability scanning events. | enable |
| oversized {enable disable} | Enable or disable logging of oversized files in the antivirus log. This field is available when virus is enabled. | enable |
| scanerror {enable disable} | Enable or disable logging of antivirus error messages. | enable |
| severity {alert critical debug emergency error information notification warning} | <p>Select the logging severity level. The FortiGate unit logs all messages at and above the logging severity level you select. For example, if you select error, the unit logs error, critical, alert and emergency level messages.</p> <p>emergency - The system is unusable.</p> <p>alert - Immediate action is required.</p> <p>critical - Functionality is affected.</p> <p>error - An erroneous condition exists and functionality is probably affected.</p> <p>warning - Functionality might be affected.</p> <p>notification - Information about normal events.</p> <p>information - General information about system operations.</p> <p>debug - Information used for diagnosing or debugging the FortiGate unit.</p> | information |

| Variable | Description | Default |
|--|--|---------|
| signature {enable disable} | Enable or disable logging of detected and prevented attacks based on the attack signature, and the action taken by the FortiGate unit, in the attack log. This field is available when <code>attack</code> is enabled. | enable |
| suspicious {enable disable} | Enable or disable logging of virus suspicious messages. | enable |
| switching-protocols {enable disable} | Enable or disable logging of protocol switching. | enable |
| traffic {enable disable} | Enable or disable the traffic log. | enable |
| url-filter {enable disable} | Enable or disable logging of blocked URLs (specified in the URL block list) in the web filter log. This field is available when <code>web</code> is enabled. | enable |
| virus {enable disable} | Enable or disable the antivirus log. | enable |
| voip {enable disable} | Enable or disable logging of VOIP messages. | enable |
| vulnerability {enable disable} | Enable or disable logging of netscan vulnerability events. | enable |
| web {enable disable} | Enable or disable the web filter log. | enable |
| web-content {enable disable} | Enable or disable logging of blocked content (specified in the banned words list) in the web filter log. This field is available when <code>web</code> is enabled. | enable |
| web-filter-activex {enable disable} | Enable or disable the logging of Active X block messages. | enable |
| web-filter-applet {enable disable} | Enable or disable the logging of java applet block messages. | enable |
| web-filter-command-block {enable disable} | Enable or disable the logging of web filter command block messages. | enable |
| web-filter-cookie {enable disable} | Enable or disable the logging of cookie block messages. | enable |
| web-filter-ftgd-quota {enable disable} | Enable or disable logging FortiGuard quota levels. | enable |
| web-filter-ftgd-quota-counting {enable disable} | Enable or disable logging FortiGuard quota counting messages. | enable |
| web-filter-ftgd-quota-expired {enable disable} | Enable or disable logging FortiGuard quota expired messages. | enable |
| web-filter-script-other {enable disable} | Enable or disable logging of other script filter messages. | enable |

disk setting

Use this command to configure log settings for logging to the local disk. Disk logging is only available for FortiGate units with an internal hard disk. You can also use this command to configure the FortiGate unit to upload current log files to an FTP server every time the log files are rolled.

If you have an AMC disk installed on your FortiGate unit, you can use `disk setting` to configure logging of traffic to the AMC disk. The AMC disk behaves as a local disk after being inserted into the FortiGate unit and the FortiGate unit rebooted. You can view logs from `Log&Report > Log Access > Disk` when logging to an AMC disk.

You can also use this command to enable SQL logs for different log types. SQL logs are stored in an SQLite database format. The main advantage of SQL log format is that it supports enhanced reports. For information about the report commands, see [“report” on page 321](#):



AMC disk is supported on all FortiGate units that have single-width AMC slots.

Syntax

```
config log disk setting
    set status {enable | disable}
    set diskfull {nolog | overwrite}
    set dlp-archive-quota <integer>
    set drive-standby-time <0-19800>
    set full-first-warning threshold
    set full-second-warning threshold
    set full-final-warning threshold
    set ips-archive {enable | disable}
    set log-quota <integer>
    set maximum-log-age <days_int>
    set max-log-file-size <integer max>
    set max-policy-packet-capture-size <size_int>
    set report {enable | disable}
    set report-quota <integer>
    set roll-schedule {daily | weekly}
    set roll-time <hh:mm>
    set source-ip <address_ipv4>
    set storage <name>
    set upload {enable | disable}
    set upload-delete-files {enable | disable}
    set upload-destination {ftp-server}
    set upload-ssl-conn {default | high | low | disable}
    set uploadaddir <dir_name_str>
    set uploadip <class_ip>
    set uploadpass <passwd>
```

```

set uploadport <port_integer>
set uploadsched {enable | disable}
set uploadtime <hour_integer>
set uploadtype {attack event im spamfilter traffic virus voip
webfilter}
set uploaduser <user_str>
set uploadzip {enable | disable}
end

```

| Variable | Description | Default |
|--|---|-----------|
| status {enable disable} | Enter to either enable or disable logging to the local disk. | disable |
| diskfull {nolog overwrite} | Enter the action to take when the local disk is full. When you enter <code>nolog</code> , the FortiGate unit will stop logging; <code>overwrite</code> will begin overwriting the oldest file once the local disk is full. | overwrite |
| dlp-archive-quota <integer> | Enter the amount (in MB) of disk space allocated for DLP logs. | 0 |
| drive-standby-time <0-19800> | Set the power management for the hard disk. Enter the number of seconds, up to 19800. If there is no hard disk activity within the defined time frame, the hard disk will spin down to conserve energy. Setting the value to 0 disables the setting. | 0 |
| full-first-warning threshold | Enter to configure the first warning before reaching the threshold. You can enter a number between 1 and 100. | 75 |
| full-second-warning threshold | Enter to configure the second warning before reaching the threshold. You can enter a number between 1 and 100. | 90 |
| full-final-warning threshold | Enter to configure the final warning before reaching the threshold. You can enter a number between 1 and 100. | 95 |
| ips-archive {enable disable} | Enable IPS packet archive logs. | enable |
| log-quota <integer> | Enter the amount (in MB) of disk space allocated for disk logging. | 0 |
| maximum-log-age <days_int> | Enter the maximum age for logs. Logs older than this are purged. | 7 |
| max-log-file-size <integer max> | Enter the maximum size of the log file (in MB) that is saved to the local disk. When the log file reaches the specified maximum size, the FortiGate unit saves the current log file and starts a new active log file. The default minimum log file size is 1 MB and the maximum log file size allowed is 1024MB. | 100 |
| max-policy-packet- capture-size <size_int> | Enter the maximum packet capture size in firewall policies. | 10 |
| report {enable disable} | Enable or disable reports. | enable |
| report-quota <integer> | Enter the amount (in MB) of disk space allocated for report logs. | 0 |

| Variable | Description | Default |
|--|--|-------------|
| roll-schedule {daily weekly} | Enter the frequency of log rolling. When set, the FortiGate unit will roll the log event if the maximum size has not been reached. | daily |
| roll-time <hh:mm> | Enter the time of day, in the format hh:mm, when the FortiGate unit saves the current log file and starts a new active log file. | 00:00 |
| source-ip <address_ipv4> | Enter the source IP address of the disk log uploading. | 0.0.0.0 |
| storage <name> | Enter a name for the storage log file. This option is only available when the current vdom is the management vdom. | |
| upload {enable disable} | <p>Enable or disable uploading log files to a remote directory. Enable <code>upload</code> to upload log files to an FTP server whenever a log file rolls.</p> <p>Use the <code>uploadaddir</code>, <code>uploadip</code>, <code>uploadpass</code>, <code>uploadport</code>, and <code>uploaduser</code> fields to add this information required to connect to the FTP server and upload the log files to a specific location on the server.</p> <p>Use the <code>uploadtype</code> field to select the type of log files to upload.</p> <p>Use the <code>upload-delete-files</code> field to delete the files from the hard disk once the FortiGate unit completes the file transfer.</p> <p>All <code>upload</code> fields are available after enabling the <code>upload</code> command.</p> | disable |
| upload-delete-files {enable disable} | Enable or disable the removal of the log files once the FortiGate unit has uploaded the log file to the FTP server. | enable |
| upload-destination { ftp-server} | Set upload destination. FTP server is the only option. | ftp-server |
| upload-ssl-conn {default high low disable} | <p>Set encryption strength for communications between the FortiGate unit and FortiAnalyzer. Available when <code>upload-destination</code> is <code>fortianalyzer</code>.</p> <p>high — use SSL with 128-bit and larger key length algorithms: DHE-RSA-AES256-SHA, AES256-SHA, EDH-RSA-DES-CBC3-SHA, DES-CBC3-SHA, DES-CBC3-MD5, DHE-RSA-AES128-SHA, AES128-SHA</p> <p>low — use SSL with 64-bit or 56-bit key length algorithms without export restrictions: EDH-RSA-DES-CBC-SHA, DES-CBC-SHA, DES-CBC-MD5</p> <p>default — use SSL with high strength algorithms and these medium-strength 128-bit key length algorithms: RC4-SHA, RC4-MD5, RC4-MD</p> <p>disable — disable the use of SSL.</p> | default |
| uploadaddir <dir_name_str> | Enter the name of the path on the FTP server where the log files will be transferred to. If you do not specify a remote directory, the log files are uploaded to the root directory of the FTP server. | No default. |
| uploadip <class_ip> | Enter the IP address of the FTP server. This is required. | 0.0.0.0 |

| Variable | Description | Default |
|---|--|--|
| uploadpass <passwd> | Enter the password required to connect to the FTP server. This is required. | No default. |
| uploadport <port_integer> | Enter the port number used by the FTP server. The default port is 21. Port 21 is the standard FTP port. | 21 |
| uploadsched {enable disable} | Enable log uploads at a specific time of the day. When set to disable, the FortiGate unit uploads the logs when the logs are rolled. | disable |
| uploadtime <hour_integer> | Enter the time of day (hour only) when the FortiGate unit uploads the logs. The uploadsched setting must first be set to enable. | 0 |
| uploadtype {attack event im spamfilter traffic virus voip webfilter} | Select the log files to upload to the FTP server. You can enter one or more of the log file types separated by spaces. Use a space to separate the log file types. If you want to remove a log file type from the list or add a log file type to the list, you must retype the list with the log file type removed or added. | traffic event spamfilter virus webfilter voip im |
| uploaduser <user_str> | Enter the user account for the upload to the FTP server. This is required. | No default. |
| uploadzip {enable disable} | Enter enable to compress the log files after uploading to the FTP server. If disable is entered, the log files are uploaded to the FTP server in plain text format. | disable |

eventfilter

Use this command to configure event logging.

Syntax

```
config log eventfilter
    set event {enable | disable}
    set router {enable | disable}
    set system {enable | disable}
    set user {enable | disable}
    set vpn {enable | disable}
    set wan-opt {enable | disable}
    set wireless-activity {enable | disable}
end
```

| Variable | Description | Default |
|---|---|---------|
| event {enable disable} | Log event messages. Must be enabled to make the following fields available. | enable |
| router {enable disable} | Log router activity. | enable |
| system {enable disable} | Log system activity messages, HA activity messages, CPU & memory usage, VIP realserver health monitoring, and AMC interface bypass mode messages. | enable |
| user {enable disable} | Log user authentication messages. | enable |
| vpn {enable disable} | Log IPSec negotiation messages, SSL user authentication, administration and session messages. | enable |
| wan-opt {enable disable} | Log WAN optimization messages. | enable |
| wireless-activity {enable disable} | Log wireless activity. | enable |

{fortianalyzer | syslogd} override-filter

Use this command within a VDOM to override the global configuration created with the `config log {fortianalyzer | syslogd} filter` command. The filter determines which types of log messages are sent to the FortiAnalyzer unit or syslog server. For syntax and descriptions, see “{disk | fortianalyzer | fortianalyzer2 | fortianalyzer3 | memory | syslogd | syslogd2 | syslogd3 | webtrends | fortiguard} filter” on page 279.

fortianalyzer override-setting

Use this command within a VDOM to override the global configuration created with the `config log fortianalyzer setting` command. These settings configure the connection to the FortiAnalyzer unit. For syntax and descriptions, see “[{fortianalyzer | fortianalyzer2 | fortianalyzer3} setting](#)” on page 290.



There is no
`config log fortianalyzer2 override-setting`
or
`config log fortianalyzer3 override-setting`
command.

{fortianalyzer | fortianalyzer2 | fortianalyzer3} setting

Use this command to configure the FortiGate unit to send log files to a FortiAnalyzer unit.

FortiAnalyzer units are network appliances that provide integrated log collection, analysis tools and data storage. Detailed log reports provide historical as well as current analysis of network and email activity to help identify security issues and reduce network misuse and abuse.

Using the CLI, you can send logs to up to three different FortiAnalyzer units for maximum fail-over protection of log data. After configuring logging to FortiAnalyzer units, the FortiGate unit will send the same log packets to all configured FortiAnalyzer units. Additional FortiAnalyzer units are configured using the `fortianalyzer2` and `fortianalyzer3` commands.



The FortiAnalyzer CLI commands are not cumulative. Using a syntax similar to the following is not valid:

```
config log fortianalyzer fortianalyzer2 fortianalyzer3 setting
```

Syntax

```
config log {fortianalyzer | fortianalyzer2 | fortianalyzer3} setting
    set status {enable | disable}
    set conn-timeout <seconds>
    set encrypt {enable | disable}
    set enc-algorithm {default | high | low | disable}
    set gui-display {enable | disable}
    set ips-archive {enable | disable}
    set localid <identifier>
    set monitor-keepalive-period <int_seconds>
    set monitor-failure-retry-period <int_seconds>
    set psksecret <pre-shared_key>
    set reliable {enable | disable}
    set server <fortianalyzer_ipv4>
    set source-ip <address_ipv4>
    set upload-option {store-and-upload | realtime}
    set upload-interval {daily | weekly | monthly}
    set upload-day <1-31> |
        {sunday | monday | tuesday | wednesday | thursday | friday |
        saturday}
    set upload-time <hh:mm>
end
```

| Variable | Description | Default |
|---------------------------|--|---------|
| status {enable disable} | Enable or disable communication with the FortiAnalyzer unit. The other fields are available only if <code>status</code> is set to <code>enable</code> . | disable |
| conn-timeout <seconds> | Enter the number of seconds before the FortiAnalyzer connection times out. | 10 |

| Variable | Description | Default |
|--|--|------------------|
| encrypt {enable disable} | Enable to use IPSec VPN tunnel for communication. When enabled, <i>enc-algorithm</i> is not available. Disable to send data as plain text over SSL with the <i>enc-algorithm</i> command. | disable |
| enc-algorithm {default high low disable} | Set encryption strength for communications between the FortiGate unit and FortiAnalyzer. high — use SSL with 128-bit and larger key length algorithms: DHE-RSA-AES256-SHA, AES256-SHA, EDH-RSA-DES-CBC3-SHA, DES-CBC3-SHA, DES-CBC3-MD5, DHE-RSA-AES128-SHA, AES128-SHA low — use SSL with 64-bit or 56-bit key length algorithms without export restrictions: EDH-RSA-DES-CBC-SHA, DES-CBC-SHA, DES-CBC-MD5 default — use SSL with high strength algorithms and these medium-strength 128-bit key length algorithms: RC4-SHA, RC4-MD5, RC4-MD disable — disable the use of SSL. | default |
| gui-display {enable disable} | Enable to display FortiAnalyzer Reports on the web-based manager. | disable |
| ips-archive {enable disable} | Enable IPS packet archive. | enable |
| localid <identifier> | Enter an identifier up to 64 characters long. You must use the same identifier on the FortiGate unit and the FortiAnalyzer unit. | No default. |
| monitor-keepalive-period <int_seconds> | Enter the interval in seconds between OFTP keepalive transmissions (for status and log buffer). Range 1 to 120. | 5 |
| monitor-failure-retry-period <int_seconds> | Enter the time in seconds between connection retries (for status and log buffer). Range 1 to 2 147 483 647. | 5 |
| psksecret <pre-shared_key> | Enter the pre-shared key for the IPSec VPN tunnel. This is needed only if <i>encrypt</i> is set to <i>enable</i> . | No default. |
| reliable {enable disable} | Enable to log to a syslog server using TCP, which ensures reliable connection setup and transmission of data. | disable |
| server <fortianalyzer_ipv4> | Enter the IP address of the FortiAnalyzer unit. This field is only available when <i>address-mode</i> is set to <i>static</i> . | 0.0.0.0 |
| source-ip <address_ipv4> | Enter the source IP address for the FortiAnalyzer, FortiAnalyzer2 and FortiAnalyzer3 units. | 0.0.0.0 |
| upload-option {store-and-upload realtime} | Choose how logs are uploaded to a FortiAnalyzer unit: realtime — Send logs directly to the FortiAnalyzer unit. store-and-upload — Log to hard disk, then upload on the schedule defined by <i>upload-interval</i> , <i>upload-day</i> and <i>upload-time</i> . You cannot switch from <i>realtime</i> to <i>store-and-upload</i> if any VDOM has disk logging disabled. | store-and-upload |

| Variable | Description | Default |
|---|---|-------------|
| upload-interval {daily weekly monthly} | Select how frequently logs are uploaded. This is available when upload-option is store-and-upload. | daily |
| upload-day <1-31> {sunday monday tuesday wednesday thursday friday saturday} | When upload-interval is monthly, enter the day of the month to upload logs. When upload-interval is weekly, select the day of the week for log uploads. This is available when upload-option is store-and-upload. | No default. |
| upload-time <hh:mm> | Enter the time of day for log uploads. This is available when upload-option is store-and-upload. | 00:59 |

fortiguard setting

Use this command for configuring FortiGuard Analysis Service settings.



The `fortiguard setting` command is only available when FortiGuard Analysis and Management Service subscription-based services are enabled. The storage space is a specified amount, and varies, depending on the services requested.

Syntax

```
config log fortiguard setting
    set enc-algorithm {default | high | low | disable}
    set quotafull {nolog | overwrite}
    set source-ip <ipv4_addr>
    set status {enable | disable}
    set upload-interval <days_int>
    set upload-option {enable | disable}
    set upload-time <hh:mm>
end
```

| Variable | Description | Default |
|--|---|-----------|
| enc-algorithm {default high low disable} | Set encryption strength for communications between the FortiGate unit and FortiAnalyzer. high — use SSL with 128-bit and larger key length algorithms: DHE-RSA-AES256-SHA, AES256-SHA, EDH-RSA-DES-CBC3-SHA, DES-CBC3-SHA, DES-CBC3-MD5, DHE-RSA-AES128-SHA, AES128-SHA low — use SSL with 64-bit or 56-bit key length algorithms without export restrictions: EDH-RSA-DES-CDBC-SHA, DES-CBC-SHA, DES-CBC-MD5 default — use SSL with high strength algorithms and these medium-strength 128-bit key length algorithms: RC4-SHA, RC4-MD5, RC4-MD disable — disable the use of SSL. | default |
| quotafull {nolog overwrite} | Enter the action to take when the specified storage space on the FortiGuard Analysis server is full. When you enter <code>nolog</code> , the FortiGate unit will stop logging, and <code>overwrite</code> will begin overwriting the oldest file. | overwrite |
| source-ip <ipv4_addr> | Enter the source IP for communications to FAMS. | 0.0.0.0 |
| status {enable disable} | Enable or disable the FortiGuard Analysis service. | disable |
| upload-interval <days_int> | Enter frequency of log upload. | |
| upload-option {enable disable} | Enable or disable logging uploading logs to FortiGuard. | disable |
| upload-time <hh:mm> | Enter time to roll logs. | |

gui-display

Use this command to configure how logs are displayed in the web-based manager.

Syntax

```
config log gui-display
  set location {memory | disk | fortianalyzer | fortiguard}
  set resolve-apps {enable | disable}
  set resolve-hosts {enable | disable}
end
```

| Variable | Description | Default |
|---|---|---------|
| location {memory disk fortianalyzer fortiguard} | Choose the location from which to display logs: memory, disk, FortiAnalyzer, or FortiGuard. | memory |
| resolve-apps {enable disable} | Enable to resolve unknown applications using the remote application database. | enable |
| resolve-hosts {enable disable} | Enable to resolve IP addresses to hostnames using reverse-DNS lookup. | enable |

memory setting

Use this command to configure log settings for logging to the FortiGate system memory.

The FortiGate system memory has a limited capacity and only displays the most recent log entries. Traffic logs are not stored in the memory buffer, due to the high volume of traffic information. After all available memory is used, by default, the FortiGate unit begins to overwrite the oldest messages. All log entries are deleted when the FortiGate unit restarts.

Syntax

```
config log memory setting
    set diskfull {overwrite}
    set status {enable | disable}
end
```

| Variable | Description | Default |
|---------------------------|--|-----------|
| diskfull {overwrite} | Enter the action to take when the memory is reaching its capacity. The only option available is <code>overwrite</code> , which means that the FortiGate unit will begin overwriting the oldest file. | overwrite |
| status {enable disable} | Enter <code>enable</code> to enable logging to the FortiGate system memory. | disable |

memory global-setting

Use this command to configure log threshold warnings, as well as the maximum buffer lines, for the FortiGate system memory.

The FortiGate system memory has a limited capacity and displays only the most recent log entries. Traffic logs are not stored in the memory buffer, due to the high volume of traffic information. After all available memory is used, by default, the FortiGate unit begins to overwrite the oldest log messages. All log entries are deleted when the FortiGate unit restarts.

Syntax

```
config log memory global-setting
    set full-final-warning-threshold
    set full-first-warning-threshold
    set full-second-warning-threshold
    set max-size <int>
end
```

| Variable | Description | Default |
|-------------------------------|---|---------|
| full-final-warning-threshold | Enter to configure the final warning before reaching the threshold. You can enter a number between 3 and 100. | 95 |
| full-first-warning-threshold | Enter to configure the first warning before reaching the threshold. You can enter a number between 1 and 98. | 75 |
| full-second-warning-threshold | Enter to configure the second warning before reaching the threshold. You can enter a number between 2 and 99. | 90 |
| max-size <int> | Enter the maximum size of the memory buffer log, in bytes. | 98304 |

setting

Use this command to configure general logging settings.

Syntax

```
config log setting
    set brief-traffic-format {enable | disable}
    set daemon-log {enable | disable}
    set fwpolicy-implicit-log {enable | disable}
    set fwpolicy6-implicit-log {enable | disable}
    set gui-location <location>
    set local-in-admin {enable | disable}
    set local-in-allow {enable | disable}
    set local-in-deny {enable | disable}
    set local-in-fortiguard {enable | disable}
    set local-in-other {enable | disable}
    set local-out {enable | disable}
    set log-invalid-packet {enable | disable}
    set log-user-in-upper {enable | disable}
    set neighbor-event {enable | disable}
    set resolve-ip {enable | disable}
    set resolve-port {enable | disable}
    set user-anonymize {enable | disable}
end
```

| Variable | Description | Default |
|--|--|------------|
| brief-traffic-format {enable disable} | Use brief format for traffic log. | disable |
| daemon-log {enable disable} | Collect daemon log. | disable |
| fwpolicy-implicit-log {enable disable} | Collect firewall implicit policy log. | disable |
| fwpolicy6-implicit-log {enable disable} | Collect firewall implicit policy6 log. | disable |
| gui-location <location> | Set which logs to display: disk, fortianalyzer, fortiguard, or memory. | fortiguard |
| local-in-admin {enable disable} | Collect local-in policy admin access log. | enable |
| local-in-allow {enable disable} | Collect local-in policy accepted log. | enable |
| local-in-deny {enable disable} | Collect local-in policy dropped log. | enable |
| local-in-fortiguard {enable disable} | Collect local-in policy FortiGuard log. | enable |
| local-in-other {enable disable} | Collect local-in-other policy log. | enable |
| local-out {enable disable} | Collect local-out log. | disable |

| Variable | Description | Default |
|--|--|---------|
| log-invalid-packet { enable disable } | <p>Enable ICSA compliant logs for the VDOM. Independent of traffic log settings, traffic log entries are generated:</p> <ul style="list-style-type: none"> • for all dropped ICMP packets • for all dropped invalid IP packets (see "check-protocol-header {loose strict}" on page 530, "anti-replay {disable loose strict}" on page 528, and "check-reset-range {disable strict}" on page 531. • for session start and on session deletion <p>This setting is not rate limited. A large volume of invalid packets can dramatically increase the number of log entries, affecting device performance.</p> | disable |
| log-user-in-upper { enable disable } | Collect log with user-in-upper. | disable |
| neighbor-event { enable disable } | Collect neighbor-event log (ARP and IPv6 neighbor discovery events). | disable |
| resolve-ip { enable disable } | Resolve ip address in traffic log to domain name if possible. | disable |
| resolve-port { enable disable } | Resolve port number in traffic log to service name if possible. | disable |
| user-anonymize { enable disable } | Enable or disable replacing user name with "anonymous" in logs. | disable |

syslogd override-setting

Use this command within a VDOM to override the global configuration created with the `config log syslogd setting` command. These settings configure the connection to a syslog server.

Syntax

```
config log syslogd override-setting
  set override {enable | disable}
  set status {enable | disable}
  set csv {enable | disable}
  set facility {alert | audit | auth | authpriv | clock | cron
               | daemon | ftp | kernel | local0 | local1 | local2 | local3
               | local4 | local5 | local6 | local7 | lpr | mail | news | ntp
               | syslog | user | uucp}
  set port <port_integer>
  set reliable {disable | enable}
  set server <address_ipv4 | fqdn>
  set source-ip <address_ipv4>
end
```

| Variable | Description | Default |
|-----------------------------|--|---------|
| override {enable disable} | Enable to use the override settings below. Disable to use the global configuration created with the <code>config log syslogd setting</code> command. | disable |
| status {enable disable} | Enter <code>enable</code> to enable logging to a remote syslog server. | disable |
| csv {enable disable} | Enter <code>enable</code> to enable the FortiGate unit to produce the log in Comma Separated Value (CSV) format. If you do not enable CSV format the FortiGate unit produces plain text files. | disable |

| Variable | Description | Default |
|--|---|-------------|
| facility {alert audit auth authpriv clock cron daemon ftp kernel local0 local1 local2 local3 local4 local5 local6 local7 lpr mail news ntp syslog user uucp} | <p>Enter the facility type. <code>facility</code> identifies the source of the log message to syslog. You might want to change <code>facility</code> to distinguish log messages from different FortiGate units. Available facility types are:</p> <ul style="list-style-type: none"> • <code>alert</code>: log alert • <code>audit</code>: log audit • <code>auth</code>: security/authorization messages • <code>authpriv</code>: security/authorization messages (private) • <code>clock</code>: clock daemon • <code>cron</code>: cron daemon performing scheduled commands • <code>daemon</code>: system daemons running background system processes • <code>ftp</code>: File Transfer Protocol (FTP) daemon • <code>kernel</code>: kernel messages • <code>local0</code> – <code>local7</code>: reserved for local use • <code>lpr</code>: line printer subsystem • <code>mail</code>: email system • <code>news</code>: network news subsystem • <code>ntp</code>: Network Time Protocol (NTP) daemon • <code>syslog</code>: messages generated internally by the syslog daemon | local7 |
| port <port_integer> | Enter the port number for communication with the syslog server. | 514 |
| reliable {disable enable} | Enable reliable delivery of syslog messages to the syslog server. When enabled, the FortiGate unit implements the RAW profile of RFC 3195 , sending log messages using TCP protocol. | disable |
| server <address_ipv4 fqdn> | Enter the IP address of the syslog server that stores the logs. | No default. |
| source-ip <address_ipv4> | Enter source IP address for syslogd, syslog2 and syslog3 | 0.0.0.0 |

{syslogd | syslogd2 | syslogd3} setting

Use this command to configure log settings for logging to a remote syslog server. You can configure the FortiGate unit to send logs to a remote computer running a syslog server.

Using the CLI, you can send logs to up to three different syslog servers. Configure additional syslog servers using `syslogd2` and `syslogd3` commands and the same fields outlined below.



Syslog CLI commands are not cumulative. Using a syntax similar to the following is not valid:

```
config log syslogd syslogd2 syslogd3 setting
```

Syntax

```
config log {syslogd | syslogd2 | syslogd3} setting
  set status {enable | disable}
  set csv {enable | disable}
  set facility {alert | audit | auth | authpriv | clock | cron |
    daemon | ftp | kernel | local0 | local1 | local2 | local3 |
    local4 | local5 | local6 | local7 | lpr | mail | news | ntp |
    syslog | user | uucp}
  set port <port_integer>
  set reliable {enable | disable}
  set server <address_ipv4 | FQDN>
  set source-ip <address_ipv4>
end
```

| Variable | Description | Default |
|---------------------------|--|---------|
| status {enable disable} | Enter <code>enable</code> to enable logging to a remote syslog server. | disable |
| csv {enable disable} | Enter <code>enable</code> to enable the FortiGate unit to produce the log in Comma Separated Value (CSV) format. If you do not enable CSV format the FortiGate unit produces plain text files. | disable |

| Variable | Description | Default |
|--|---|-------------|
| facility {alert audit auth authpriv clock cron daemon ftp kernel local0 local1 local2 local3 local4 local5 local6 local7 lpr mail news ntp syslog user uucp} | <p>Enter the facility type. <code>facility</code> identifies the source of the log message to syslog. You might want to change <code>facility</code> to distinguish log messages from different FortiGate units. Available facility types are:</p> <ul style="list-style-type: none"> • <code>alert</code>: log alert • <code>audit</code>: log audit • <code>auth</code>: security/authorization messages • <code>authpriv</code>: security/authorization messages (private) • <code>clock</code>: clock daemon • <code>cron</code>: cron daemon performing scheduled commands • <code>daemon</code>: system daemons running background system processes • <code>ftp</code>: File Transfer Protocol (FTP) daemon • <code>kernel</code>: kernel messages • <code>local0</code> – <code>local7</code>: reserved for local use • <code>lpr</code>: line printer subsystem • <code>mail</code>: email system • <code>news</code>: network news subsystem • <code>ntp</code>: Network Time Protocol (NTP) daemon • <code>syslog</code>: messages generated internally by the syslog daemon | local7 |
| port <port_integer> | Enter the port number for communication with the syslog server. | 514 |
| reliable {enable disable} | <p>Enable reliable delivery of syslog messages to the syslog server. When enabled, the FortiGate unit implements the RAW profile of RFC 3195 for reliable delivery of log messages to the syslog server.</p> <p>Reliable syslog protects log information through authentication and data encryption and ensures that the log messages are reliably delivered in the correct order.</p> | disable |
| server <address_ipv4 FQDN> | <p>Enter the IP address of the syslog server that stores the logs.</p> <p>Host names must comply with RFC1035.</p> | No default. |
| source-ip <address_ipv4> | Enter source IP address for syslogd, syslog2 and syslog3 | 0.0.0.0 |

webtrends setting

Use this command to configure log settings for logging to a remote computer running a NetIQ WebTrends firewall reporting server.

FortiGate log formats comply with WebTrends Enhanced Log Format (WELF) and are compatible with NetIQ WebTrends Security Reporting Center and Firewall Suite 4.1.

Syntax

```
config log webtrends setting
    set server <address_ipv4>
    set status {enable | disable}
end
```

| Variable | Description | Default |
|---------------------------|--|-------------|
| server <address_ipv4> | Enter the IP address of the WebTrends server that stores the logs. | No default. |
| status {enable disable} | Enter <code>enable</code> to enable logging to a WebTrends server. | disable |

netscan

Use these commands to configure the Endpoint network vulnerability scanner.

[assets](#)

[settings](#)



Note: Vulnerability scanning is not available in Transparent mode.

assets

Use this command to define assets (network devices and networks) to run network vulnerability scans on.

Syntax

```
config netscan assets
edit <asset_id_int>
    set addr-type {ip | range}
    set auth-unix {enable | disable}
    set auth-windows {enable | disable}
    set mode {discovery | scan}
    set name <string>
    set scheduled {enable | disable}
    set start-ip <address_ipv4>
    set end-ip <address_ipv4>
    set unix-password <pass_str>
    set unix-username <id_str>
    set win-password <pass_str>
    set win-username <id_str>
end
```

| Variables | Description | Default |
|------------------------------------|--|---------|
| <asset_id_int> | Enter the unique ID number for this asset. | |
| addr-type {ip range} | Select ip to scan a single IP address. Select range to scan a range of IP addresses. Note: You cannot specify authentication parameters for an address range. | ip |
| auth-unix {enable disable} | Enable to allow the FortiGate unit to authenticate with a unix host during the vulnerability scan. If you enable this option you must enter a unix-username and a unix-password . | disable |
| auth-windows {enable disable} | Enable to allow the FortiGate unit to authenticate with a Windows host during the vulnerability scan. If you enable this option you must enter a win-username and a win-password . | disable |
| mode {discovery scan} | Select discovery to find assets with the specified IP address or address range. | scan |
| name <string> | Enter an name of the asset. | |
| scheduled {enable disable} | Enable or disable including this asset in scheduled scans. | enable |
| start-ip <address_ipv4> | Enter the IP address of the asset to scan. If addr-type is set to range enter the first IP address in the IP address range to scan. | 0.0.0.0 |
| end-ip <address_ipv4> | If addr-type is set to range enter the last IP address in the IP address range to scan. | 0.0.0.0 |
| unix-password <pass_str> | Enter the password the FortiAnalyzer uses to authenticate with the UNIX host. This command appears only when auth is set to unix . | |

| Variables | Description | Default |
|----------------------------|---|---------|
| unix-username <id_str> | Enter the username the FortiAnalyzer uses to authenticate with the UNIX host. This command appears only when <code>auth</code> is set to <code>unix</code> . | |
| win-password <pass_str> | Enter the password the FortiAnalyzer uses to authenticate with the Windows host. | |
| win-username <id_str> | Enter the username the FortiAnalyzer uses to authenticate with the Windows host. | |

settings

Use this command to configure network vulnerability scanner settings that control when scans are run.

Syntax

```
config netscan settings
  set day-of-month <day_int>
  set day-of-week {monday | tuesday | wednesday | thursday | friday |
    saturday | sunday}
  set os-detection {enable | disable | auto}
  set pause-from <time_str>
  set pause-to <time_str>
  set recurrence {daily | monthly | weekly}
  set scan-mode {full | quick | standard}
  set scheduled-pause {enable | disable | default}
  set service-detection {enable | disable | auto}
  set tcp-scan {enable | disable | auto}
  set time <hh:mm>
  set udp-scan {enable | disable | auto}
end
```

| Variables | Description | Default |
|--|---|---------|
| day-of-month <day_int> | Enter the day of the month on which to run scans. You can only select one day. This option is only available if <code>schedule</code> is enabled and <code>recurrence</code> is monthly. | 1 |
| day-of-week {monday tuesday wednesday thursday friday saturday sunday} | Select the day of the week on which to run scans. You can only select one day. This option is only available if <code>schedule</code> is enabled and <code>recurrence</code> is weekly. | sunday |
| os-detection {enable disable auto} | Enable or disable host operating system detection, or select <code>auto</code> to use the default setting for this type of scan. | auto |
| pause-from <time_str> | Enter the time, in hh:mm format, when network scanning pause begins. | 00:00 |
| pause-to <time_str> | Enter the time, in hh:mm format, when network scanning pause ends. | 00:00 |
| recurrence {daily monthly weekly} | Set scheduled scans to run once a day, once a month, or once a week. | weekly |
| scan-mode {full quick standard} | Specify the scan mode to use: full — scan all TCP and UDP ports quick — perform a quick scan of commonly used TCP and UDP ports standard — perform a standard scan of more ports than the quick scan but not all ports. | quick |
| scheduled-pause {enable disable default} | Enable or disable scheduled pause in network scanning, or use default setting. | default |

| Variables | Description | Default |
|--|---|---------|
| service-detection { enable disable auto } | Enable or disable explicit service detection, or select <code>auto</code> to use the default setting for this type of scan. | auto |
| tcp-scan { enable disable auto } | Enable or disable TCP scan, or select <code>auto</code> to use the default setting for this type of scan. | auto |
| time <hh:mm> | Enter the time of day on which to start a scan. | 00:00 |
| udp-scan { enable disable auto } | Enable or disable UDP scan, or select <code>auto</code> to use the default setting for this type of scan. | auto |

pbx

Use the `config pbx` command to configure PBX feature of the FortiGate Voice unit.

This chapter describes the following commands:

`dialplan`

`did`

`extension`

`global`

`ringgrp`

`voice-menu`

`sip-trunk`

dialplan

Use this command to add a dial plan and add rules to the dial plan. A dial plan rule indicates an outgoing destination to send calls to. You can add multiple rules to a dial plan. You add dial plans to extensions to control how to handle outgoing calls from the extension.

Syntax

```
config pbx dialplan
  edit <pbx_dialplan_name>
    set comments <comment_string>
    config rule
      edit <rule_name_str>
        set action {allow | block}
        set callthrough {fxo1 | fxo2 | fxo3 | fx04
          | <voip_providers>}
        set outgoing-prefix <pattern_str>
        set phone-no-beginwith <patern_str>
        set prepend <pattern_str>
        set use-global-outgoing-prefix {no | yes}
      end
    end
  end
```

| Variables | Description | Default |
|--|---|------------|
| edit <pbx_dialplan_name> | Enter the name for the dial plan. If you entering an existing dial plan, select Tab to get to the dial plan that you want to edit. | No default |
| comments <comment_string> | Optionally enter a description of the dial plan. | No default |
| config rule | Configure a new dial plan rule. | No default |
| edit <rule_name_str> | Enter the name of the dial plan rule to configure. | No default |
| action {allow block} | Set the action to <code>allow</code> if this dial plan rule should allow a call. Set the action to <code>block</code> if the dial plan should block a call. For example, if you want to block international calls you could set the Phone Number begin with to 011 and set the action to block. | No default |
| callthrough {fxo1 fxo2 fxo3 fx04 <voip_providers>} | Select one or more destinations that the dial plan rule sends outgoing calls to. <code>fxo1</code> , <code>fxo2</code> , <code>fxo3</code> , and <code>fx04</code> are the 4 PSTN interfaces. <code><voip_providers></code> are the VoIP providers added to the FortiGate Voice. A dial plan rule can send calls to one or more destinations. | No default |
| outgoing-prefix <pattern_str> | If you set <code>use-global-outgoing-prefix</code> to <code>no</code> you can enter a different outgoing prefix for this dial plan. | null |
| phone-no-beginwith <patern_str> | Enter the leading digits of the phone number that this dial plan rule should match with. For example, a dial plan rule for toll free numbers in North America should begin with 18. The FortiGate Voice uses a best match to match a dialed number with a dial plan. So each dial plan should have a different Phone number Begin with setting. But you should plan your dial plan to make sure that unexpected matches do not occur. | null |

| Variables | Description | Default |
|--|---|---------|
| prepend <pattern_str> | Add digits that should be prepended or added to the beginning of the dialed number before the call is forwarded to its destination. You can prepend digits at the beginning of a call if special dialing is required to reach an external phone system. | null |
| use-global-outgoing-prefix {no yes} | Select <i>yes</i> if the dial plan rule should use the default outgoing prefix (usually 9). Select <i>no</i> to add a different outgoing-prefix. | yes |

did

Use this command to configure Direct Inward Dialing (DID). DID allows calls from external phone systems to dial directly to extensions added to the FortiGate Voice unit.

Syntax

```
config pbx did
  edit <pbx_did_name>
    set external-line {fxo1 | fxo2 | fxo3 | fx04 | <voip_providers>}
    set cid-number <phone_number>
    set extension <extension_number>
    set comment <comment_string>
  end
```

| Variables | Description | Default |
|--|--|-------------|
| edit <pbx_did_name> | Enter the name for the Direct Inward Dial. | No default. |
| external-line {fxo1 fxo2 fxo3 fx04 <voip_providers>} | Select one external system that can dial directly to an extension. fxo1, fxo2, fxo3, and fx04 are the 4 PSTN interfaces. <voip_providers> are the VoIP providers added to the FortiGate Voice. | null |
| cid-number <phone_number> | Enter the phone number dialed by a caller on the external system. | null |
| extension <extension_number> | Enter the FortiGate Voice extension number the call is directed to. | null |
| comment <comment_string> | Enter a description, if applicable, about the direct inward dial configuration. | null |

extension

Use this command to add SIP phone extensions to the FortiGate Voice unit. You can add new extensions or reconfigure the existing ones. For example, you can label an extension by user name, or you can add an extension and set it as a host for conference calls, or you can get FortiGate Voice unit to send email notifications to the users when they receive new voicemail messages.



FortiGate Voice unit uses the alertmail settings to access an SMTP server and send email notifications. Alertmail can be configured through `config system alertmail` command. For more information about alertmail CLI command configuration refer to FortiGate CLI Reference.

Syntax

```
config pbx extension
  edit <extension_number>
    set attach {enable | disable}
    set auto-delete {enable | disable}
    set conference-host <extension_number>
    set dialplan <dialplan_name>
    set email <user_email>
    set email-notify {enable | disable}
    set first-name <first_name>
    set host-pin <host_password>
    set last-name <surname_name>
    set macaddress <mac_address>
    set max-msg <max_messages_allowed>
    set nat {no | yes}
    set recordable-flag {enable | disable}
    set secret <user_password>
    set type {conference | sip-phone}
    set video {enable | disable}
    set vm-secret <user_password>
    set voicemail {enable | disable}
  end
```

| Variables | Description | Default |
|------------------------------------|---|-------------|
| edit <extension_number> | Enter the extension number. The extension number has to match the <code>config pbx global</code> extension pattern. | No default. |
| attach {enable disable} | Enable the voicemail message as an attachment in an email. | disable |
| auto-delete {enable disable} | Enable to automatically delete voice mail. | disable |
| conference-host <extension_number> | Enter the extension number that will host the conference. | null |
| dialplan <dialplan_name> | Enter the dial plan that you want to use for the extension. | null |

| Variables | Description | Default |
|---------------------------------------|--|-----------------------|
| email <user_email> | Enter the user's email address. This email address can be used to notify the user when they have a new voicemail message. | null |
| email-notify {enable disable} | Enable email notification. When email notification is enabled the user gets notified of each new voicemail messages. | disable |
| first-name <first_name> | Enter the person's first name. | null |
| host-pin <host_password> | Enter the password for the conference call. The password must contain only numbers. The users need to enter this password to join the conference call. | |
| last-name <surname_name> | Enter the surname of the person. | null |
| macaddress <mac_address> | Enter the MAC address of the SIP phone for the current extension. A typical MAC address consists of six double digit alpha-numeric characters separated by colons. Colons must be used when entering the MAC address. | 00:00:00: 00:00:00 |
| max-msg <max_messages_allowed> | Enter the maximum number of voicemail messages that are allowed in a user's voicemail inbox. | 50 |
| nat {no yes} | Enter to indicate that the phone is behind a NAT device. | no |
| recordable-flag {enable disable} | Enable conference recording. When enabled the conference call are recorded on FortiGate Voice unit's hard drive. | disable |
| secret <user_password> | Enter the user's password for voicemail. | No default. |
| type {conference sip-phone} | Enter the type of extension to configure. sip-phone to configure a SIP phone extension conference to add a conference bridge. Multiple users can call the conference bridge extension number enter the <code>secret</code> and have a conference call. A conference bridge only requires an extension number and a <code>secret</code> . | sip-phone |
| video {enable disable} | Enable video conferencing. | disable |
| vm-secret <user_password> | Enter the user's password for accessing their voicemail inbox. | No default. |
| voicemail {enable disable} | Enable the extension to have voicemail. | enable |

global

Use this command to configure voicemail settings such as limiting the length of voicemail messages, as well as the country and the extension pattern of the user.

Syntax

```
config pbx global
  set atxfer-dtmf <str>
  set blindxfer-dtmf <str>
  set block-blacklist {enable | disable}
  set code-callpark <str>
  set country-area <country_name>
  set country-code <country_code>
  set dtmf-callpark <str>
  set efax-check-interval <integer>
  set extension-pattern <extension_pattern>
  set fax-admin-email <email_address>
  set ftgd-voice-server <server_address>
  set local-area-code <code_string>
  set max-voicemail <max_length_seconds>
  set outgoing-prefix <pattern_str>
  set parking-slots <int>
  set parking-time <int>
  set ring-timeout <time_int>
  set rtp-hold-timeout <time_int>
  set rtp-timeout <time_int>
  set voicemail-extension <access_number>
end
```

| Variables | Description | Default |
|------------------------------------|--|---------|
| atxfer-dtmf <str> | The DTMF command to trigger an attended transfer. | *2 |
| blindxfer-dtmf <str> | The DTMF command to trigger a blind transfer. | #1 |
| block-blacklist {enable disable} | Enable to block blacklist IP addresses. | enable |
| code-callpark <str> | Enter this numeric code to park the current call. | 700 |
| country-area <country_name> | Enter the name of the country in which the FortiGate Voice unit is installed. | USA |
| country-code <country_code> | Enter the country code in which the FortiGate Voice unit is installed. | 1 |
| dtmf-callpark <str> | The DTMF command to trigger a call park. | #72 |
| efax-check-interval <integer> | Enter the efax polling interval from FortiGuard fax server. The value range is 5 to 120 in minutes. | 5 |

| Variables | Description | Default |
|--|---|------------------------|
| extension-pattern <extension_pattern> | <p>Enter a pattern that defines the valid extensions that can be added to the FortiGate Voice configuration. The pattern can include numbers that must be in every extension and upper case Xs to indicate the number of digits. The extension range can only contain numbers and the letter X.</p> <p>If you add numbers to the extension range, all extensions added to this FortiGate Voice unit must include the same numbers in the same location in the extension number. For example, if you include a 6 as the first digit, all extensions added this FortiGate Voice unit must begin with the number 6.</p> <p>The Xs indicate the number of digits in addition to the required number that each extension must have. For example, 6XXX indicates the extensions must start with the number 6 and be followed by any three numbers.</p> <p>Usually you would add one or two numbers to the start of the extension range to identify the extensions for this PBX and follow this with enough Xs to be able to add the required number of extensions.</p> <p>The extension range should not begin with the same number as the outgoing prefix.</p> | null |
| fax-admin-email <email_address> | Enter the email address of the fax administrator. | null |
| ftgd-voice-server <server_address> | Enter the FortiGuard voice server address. | service.fortivoice.com |
| local-area-code <code_string> | Enter the local area code for the country or region in which you are installing the FortiGate Voice unit. | 408 |
| max-voicemail <max_length_seconds> | Limit the length of voicemail messages in seconds. Set to 0 for no limit. | 60 |
| outgoing-prefix <pattern_str> | The number that PBX users must dial to get an outside line. For example, if users should dial 9 to get an outside line, add 9 to this field. The outgoing prefix should not be the same as the first number of the extension range. | 9 |
| parking-slots <int> | The maximum number of calls that can be parked at the same time. | 20 |
| parking-time <int> | The length of time, in seconds, a call can be parked. If this time expires without the call being answered, the parked call will ring back to the extension from which it was parked. | 45 |
| ring-timeout <time_int> | The number of seconds that an extension should be allowed to ring before going to voicemail. | 20 |
| rtp-hold-timeout <time_int> | The amount of time in seconds that the extension will wait on hold for RTP packets before hanging up the call. 0 means no time limit. | 0 |
| rtp-timeout <time_int> | The amount of time in seconds during an active call that the extension will wait for RTP packets before hanging up the call. 0 means no time limit. | 60 |
| voicemail-extension <access_number> | Enter the voicemail extension number that a user will use to access their voicemail inbox. | *97 |

ringgrp

Use this command to add and configure the extension groups. An extension group here is referred to a ring group and is a group of extensions that can be called using one number. You can configure the ring group to call all of the extensions in the group at the same time or to call the extensions one at a time until someone answers.



The order in which the members are added to the ring group does not match the order in which the FortiGate Voice unit calls them.

Syntax

```
config pbx ringgrp
  edit <ring_group_name>
    set description <description_str>
    set member <acd_group_member>
    set no-answer-action {hangup | ivr | voicemail}
    set strategy {ring-all | sequential}
    set voicemail-of-extension <extension_number>
  end
```

| Variables | Description | Default |
|--|---|-------------|
| edit <ring_group_name> | Enter the name for the group. | No default. |
| description <description_str> | A description of the extension group. | null |
| member <acd_group_member> | Enter the ACD member for the group. | No default. |
| no-answer-action {hangup ivr voicemail} | Enter the action that will be taken when none of the extensions in the ring group answers. hangup — hand up and end the call. ivr — return the caller to the attendant where they can try another extension. voicemail — the caller is directed to the voicemail system where they can leave a message. | voicemail |
| strategy {ring-all sequential} | Control how the extensions in the group are called by the ring group. ring-all — calls all of the extensions in the group at the same time. sequential — calls the extensions in the group one at a time in the order in which they have been added to the group. | sequential |
| voicemail-of-extension <extension_number> | Enter the extension number to use for voicemail if no one answers the call and no-answer-action is set to voicemail. | null |

voice-menu

Use this command to configure the menu that callers will access when they call. The variable `config press-<number>` configures the settings for the type of ring group and the type of group associated with that number.

Syntax

```
config pbx voice-menu
  set comment <comment_string>
  set password <ext_password>
  set recorder-exten <extension_str>
    config [press-0 | press-1 | press-2 | press-3 | press-4 | press-
      5 | press-6 | press-7 | press-8 | press-9]
      set type {directory | none | ring-group | voicemail}
      set ring-group <group_string>
    end
  end
```

| Variables | Description | Default |
|---|--|-------------|
| comment <comment_string> | Enter a description of the voice-menu settings, if applicable. | No default. |
| password <ext_password> | Enter the password to access recording a new IVR message. | null |
| recorder-exten <extension_str> | Enter the extension number for recording a new IVR message. | *30 |
| config [press-0 press-1 press-2 press-3 press-4 press-5 press-6 press-7 press-8 press-9] | Use this command when configuring what action each number on the phone's keypad will take. For example, you want the personnel directory to come up every time someone presses 1; <code>config press-1</code> variable would have the type <code>directory</code> selected in <code>type</code> . | No default. |
| type {directory none ring-group voicemail} | Enter the type of action that is associated with the specific number on the phone's keypad. For example, the office phone directory is heard when a caller presses 0 because <code>config press-0</code> has <code>directory</code> as its type. | No default. |
| ring-group <group_string> | Enter to include a specific ring-group if you have select <code>ring-group</code> in <code>type</code> . This variable appears only when <code>ring-group</code> is selected in <code>type</code> . | null |

sip-trunk

Use this command to configure SIP server providers for the PBX. If your FortiGate Voice unit is installed in North America and the Country Code is set to 1 then you can use the FortiGuard Voice service as your SIP service provider. (The default Country Code is 1. To change the country code, see [“pbx global” on page 315](#).) The FortiGuard Voice service is supported only in North America. If you install the FortiGate Voice unit elsewhere in the world and change the Country Code, the FortiGuard Voice Service configuration is replaced by the SIP trunk configuration. You can use the SIP trunk configuration to add one or more SIP service providers to the FortiGate Voice configuration.

Syntax

```
config pbx voip-provider
  edit <provider_name>
    set user <user_name>
    set domain {<VoIP_provider_address_ipv4>
      | <VoIP_provider_domain> }
    set secret <password>
    set authuser <authuser>
    set display-name <display_name>
    set registration-interval <refresh_interval>
    set account-type {static | dynamic}
    set dtmf-metod {auto | inband | info | rfc2833}
    set codec {alaw | g729 | none | ulaw}
    set codec1 {alaw | g729 | none | ulaw}
    set codec2 {alaw | g729 | none | ulaw}
    set video {enable | disable}
  end
```

| Variables | Description | Default |
|---|---|-------------|
| edit <provider_name> | Enter the VoIP provider's name. | No default |
| user <user_name> | Enter the user name for the provider. You can enter the phone number registered with this provider instead. | No default |
| secret <password> | Enter the password associated with the provider. | No default |
| domain {<VoIP_provider_address_ipv4> <VoIP_provider_domain> } | The VoIP provider's domain name or IP address. For example, 172.20.120.11 or voip.example.com. | No default |
| authuser <authuser> | Enter the authentication user for the account. | No default |
| display-name <display_name> | Enter the name that will be used as the caller ID name if the provider supports this feature. | No default |
| registration-interval <refresh_interval> | Enter a number for the refresh interval. | No default |
| account-type {static dynamic} | Enter to define the type of account. | No default. |
| dtmf-metod {auto inband info rfc2833} | Enter the DTMF method that will be used. | No default |
| codec {alaw g729 none ulaw} | Enter the most preferred Codec for the VoIP provider. | ulaw |

| Variables | Description | Default |
|---------------------------------------|--|---------|
| codec1 {alaw g729 none ulaw} | Enter the second most preferred Codec for the VoIP provider. | none |
| codec2 {alaw g729 none ulaw} | Enter the third most preferred Codec for the VoIP provider. | none |
| video {enable disable} | Enable video capability if the provider supports this feature. | disable |

report

Use these commands to configure SQL reports. You can use the command `get report database schema` to display the FortiGate SQL reporting database schema.



The command descriptions in this chapter have not been completely updated for FortiOS 5.0. This chapter will be updated for a future version of this document.

[chart](#)

[dataset](#)

[layout](#)

[style](#)

[summary](#)

[theme](#)

chart

Use the following command to configure a chart or widget. You can edit the settings of existing widgets or you can add new widgets. To add a new widget you need to have a dataset for it as well as a title. You can also configure the widget to be a graph in various formats or a table and you can also optionally configure details about the appearance of the graph or table.

As you change chart format settings you can go to the Executive Summary page of the web-based manager and view the chart. Refresh your browser to see format changes. You must use the `end` command to exit from the `config report chart` command to view your changes in the widget.



Charts are called widgets in the Executive Summary on the web-based manager. In the web-based manager each widget has a name which is set using the `comments` field of the `config report chart` command. When you edit a chart you specify a chart name that is only used in the CLI. To determine the widget name of a chart you must edit it and view the `comments` setting.

Syntax



Due to the complexity and duplication in the `chart` command, the `set` commands are listed in simple alphabetical order.

```
config report chart
  edit <chart_name>
    config category-series
    config column
      edit <column_number>
        config mapping
          edit <id>
        config value-series
        config x-series
        config y-series
      end
    set background <color_hex>
    set caption <caption_str>
    set caption-font-size <size_int>
    set color-palette <palette_hex>
    set comments <comment_str>
    set databind <value_expr_str>
    set dataset <dataset_name>
    set detail-unit <unit_str>
    set detail-value <value-str>
    set dimension {2D | 3D}
    set displayname <name_str>
    set drill-down-chart <chart-name>
    set extra-databind <value_expr_str>
    set extra-y {disable | enable}
    set extra-y-legend <legend_string>
```

```

set font-size <size_int>
set footer-unit <string>
set footer-value <value_str>
set graph-type {bar | flow | line | none | pie}
set group <group_str>
set header-value <string>
set is-category {no | yes}
set label-angle {45-degree | vertical | horizontal}
set legend {enable | disable}
set legend-font-size <size_int>
set op {equal | greater | greater-equal | less | less-equal
      | none}
set period {last24 | last7d}
set scale-format {YYYY-MM-DD-HH-MM | YYYY-MM-DD | HH | YYYY-MM-
      DD | YYYY-MM | YYYY | HH-MM | MM-DD}
set scale-number-of-step <steps_int>
set scale-origin {max | min}
set scale-start {now | hh:mm yyyy/mm/dd}
set scale-step <step_int>
set scale-type datetime
set scale-unit {day | hour | minute | month | year}
set style {auto | manual}
set title <title_str>
set title-font-size <size_int>
set type {graph | table}
set unit <unit_str>
set value-type {integer | string}
set value1 {<value_int> | <value_str>}
set value2 {<value_int> | <value_str>}
set y-legend <legend_str>
end

```

| Variable | Description | Default |
|------------------------|--|---------|
| config category-series | Configure the category settings required for a pie chart. | |
| config column | Configure columns for a table. To configure these settings <code>style</code> must be <code>manual</code> and <code>type</code> must be <code>table</code> . You can add multiple columns to the table and configure settings for each column. | |
| config mapping | Configure mapping for a table. | |
| config value-series | Configure the value settings required for a pie chart. | |
| config x-series | Configure settings for the x axis of a bar or line graph. To configure these settings <code>style</code> must be <code>manual</code> and <code>type</code> must be <code>graph</code> . | |
| config y-series | Configure settings for the y axis of a bar or line graph. To configure these settings <code>style</code> must be <code>manual</code> and <code>type</code> must be <code>graph</code> . | |

| Variable | Description | Default |
|---------------------------------|--|-------------|
| <chart_name> | Enter the name of a new or existing chart. The <chart_name> only appears in the CLI. The web-based manager includes widget names that are set using the <code>comments</code> field. | |
| <column_number> | Enter the number of the column to configure. Columns are numbered from the left starting at 1. | |
| <id> | Identifies a mapping instance. | |
| background <color_hex> | Enter the hexadecimal value for an HTML color to set the background color for a graph. The color value should begin with 0x. For example, the color 0xff0000 results in a red background. | |
| caption <caption_str> | Add a caption text string. | |
| caption-font-size <size_int> | Set the size of the font used to display a caption. 0 means the font size is set automatically. The font size range is 5 to 20. | 0 |
| color-palette <palette_hex> | Enter the hexadecimal value for an HTML color palette. The color palette value should begin with 0x. | |
| comments <comment_str> | Enter the name of the widget. You use this name to select the widget when adding it to the Executive Summary from the web-based manager. This name appears at the top of the widget when it is displayed in the Executive Summary. | |
| databind <value_expr_str> | Enter an SQL databind value expression for binding data to the series being configured. | |
| dataset <dataset_name> | Enter the name of the dataset that provides the data for this chart. Use the <code>config report dataset</code> command to add or edit data sets. The default configuration includes a number of pre-configured data sets. | No default. |
| detail-unit <unit_str> | Enter an abbreviation to display for the measurement unit, "MB", for example. | |
| detail-value <value_str> | Define the value to appear in each column of a table. | |
| dimension {2D 3D} | Define whether bar and pie graphs will have a 2D or 3D display. | 3D |
| displayname <name_str> | Set the name to be displayed for a mapping. | |
| drill-down-chart <chart-name> | Enter the chart name to drill down into. | |
| extra-databind <value_expr_str> | Enter an SQL databind value expression for binding extra data to the series being configured. | |
| extra-y {disable enable} | Enable or disable adding a second or extra set of data to the y-axis of a graph. | disable |
| extra-y-legend <legend_string> | Add a name to a second or extra set of data added to the y-axis of a graph. | |
| font-size <size_int> | Set the size of the font used to display a title. 0 means the font size is set automatically. The font size range is 5 to 20. | 0 |
| footer-unit <string> | Enter an abbreviation to display for the footer unit, "MB", for example. | |

| Variable | Description | Default |
|---|--|---|
| footer-value <value-str> | Define the value to appear in the footer of a table. | |
| graph-type { bar flow line none pie } | If <code>type</code> is set to <code>graph</code> select the type of graph used to display information in the widget. | none |
| group <group_str> | Enter a group string. | |
| header-value <string> | Define the value to appear in the header of a table. | |
| is-category { no yes } | Specify whether an x axis of a graph displays categories or a series of values. | no |
| label-angle { 45-degree vertical horizontal } | Select the angle for displaying the x or y axis label. | Varies depending on the chart and series. |
| legend { enable disable } | Enable or disable the generation and display of a data legend. | enable |
| legend-font-size <size_int> | Set the size of the font used to display a legend. 0 means the font size is set automatically. The font size range is 5 to 20. | 0 |
| op { equal greater greater-equal less less-equal none } | Set the mapping option | none |
| period { last24 last7d } | Select the chart report period: last 24 hours or last seven days. | last7d |
| scale-format { YYYY-MM-DD-HH-MM YYYY-MM-DD HH YYYY-MM-DD YYYY-MM YYYY HH-MM MM-DD } | Set the format for displaying the date and time on the x-axis of a graph. | YYYY-MM-DD-HH-MM |
| scale-number-of-step <steps_int> | Set the number of steps on the horizontal axis of the graph. The range is 1 to 31. | 0 |
| scale-origin { max min } | Set the time start point and direction of time on the x-axis of the graph: max along the x-axis time is displayed in reverse starting at the origin of the graph with the <code>scale-start</code> time. min along the x-axis time is displayed in the forward direction starting at the origin of the graph with the <code>scale-start</code> time. | max |
| scale-start { now hh:mm yyyy/mm/dd } | Set the start time for the x-axis. <code>now</code> sets the start time to the time that the graph was generated. You can also specify a time and date. The year range is 2001-2050. | now |
| scale-step <step_int> | The number of <code>scale-units</code> in each x-axis scale step. | 0 |
| scale-type datetime | Only the <code>datetime</code> scale type is supported. Sets the x-axis to display dates and times. | datetime |
| scale-unit { day hour minute month year } | The units of the <code>scale-step</code> on the x-axis. | day |

| Variable | Description | Default |
|------------------------------------|---|---------|
| style {auto manual} | By default <code>style</code> is set to <code>auto</code> which means the appearance of the graph or chart in the widget is configured automatically. You can set <code>style</code> to <code>manual</code> to manually configure details about the appearance of the chart or graph in the widget. | auto |
| title <title_str> | Enter the title of the graph or table. The title is optional and appears inside the widget above the graph or chart. This is not the name of the widget. Use the <code>comments</code> field to add the title or name of the widget. | |
| title-font-size <size_int> | Set the size of the font used to display the title. 0 means the font size is set automatically. The font size range is 5 to 20. | 0 |
| type {graph table} | Configure whether this widget presents information in a graphical form as a graph or as a table of values. If you select <code>graph</code> use the <code>graph-type</code> field to configure the type of graph. | graph |
| unit <unit_str> | Enter the name of the units to be displayed on the x-axis. | |
| value-type {integer string} | Configure the mapping value to be an integer or a text string. | integer |
| value1 {<value_int> <value_str>} | Set the first mapping value. | |
| value2 {<value_int> <value_str>} | Set a second mapping value if required. | |
| y-legend <legend_str> | Add a name for the data included on the y-axis of a graph. | |

dataset

Use the following command to configure report data sets. You can configure existing data sets or add new ones.



Expert knowledge of SQL is required to write and edit data set queries.

Syntax

```
config report dataset
    edit <report_dataset>
    set query <SQL_statement>
    config field
        edit <field-id>
            set displayname <string>
            set type {text | integer | date | ip}
        end
    end
end
```

| Variable | Description | Default |
|--------------------------------------|--|---------|
| edit <report_dataset> | Enter the name of an existing dataset or a new name. Press ? to view the list of existing datasets. | |
| query <SQL_statement> | Enter the SQL statement that retrieves the required data from the database. Comprehensive knowledge of SQL queries is required. See the existing datasets for example SQL queries. | |
| config field | You should configure fields only to modify the type or displayed name of the column for use in a table or chart. | |
| edit <field-id> | Enter a field id from 1 to the number of SQL result fields in the SQL query. | |
| displayname <string> | Enter the name for the field to be displayed in tables and charts. | |
| type {text integer date ip} | Select the type of data in the field. All options are not available for all fields. | text |

layout

Use this command configure report layouts. Layouts help you define the content of your reports. You can create sub-styles for page headers, page footers and the body section of the report. You can also schedule a reporting cycle and set a specific time and day for generating reports. You can select a layout from a pre-defined list or you can create your own report layout. Once you have all layout parameters set, you can save it and use it in any report. You can use the following options to customize layouts or create new layouts.

Syntax

```
config report layout
  edit <layout name>
    set title <text>
    set cache-time-out <seconds_int>
    set cutoff-option {run-time | custom}
    set cutoff-time <time_str>
    set description <text>
    set email-recipients <recipients_str>
    set email-send {enable | disable}
    set format {html | pdf}
    set schedule-type {demand | daily | weekly}
    set time <HH:MM>
    set day {sunday | monday | tuesday | wednesday | thursday | friday
            | saturday}
    set style-theme <theme name>
    set options {include-table-of-contents | auto-numbering-heading
               | view-chart-as-heading | show-html-navbar-before-heading}
config page
  set paper{A4|letter}
  set column-break-before {heading1 | heading2 | heading3}
  set options {header-on-first-page | footer-on-first-page}
  set style <style name>
config header
  set style <style name>
config header-item
  set edit <item_id>
  set style <style name>
  set type {text | image}
  set content <text>
  set description <text>
  set img-src <text>
```



```

config footer
    set style <style name>
    config footer-item
        set edit <item_id>
        set style <style name>
        set type {text | image}
        set content <text>
        set description <text>
        set img-src <text>
    end
end
config body-item
    set edit <item_id>
    set type {text | image | chart | misc}
    set description <text>
    set style <style name>
    set text-component {heading1 | heading2 | heading3 | normal text}
    set content <text>
    set img-src <text>
    set chart <chart name>
    set chart-options {hide-title | include-no-data | show-caption}
    set misc-component {hline | page-break | column-break | section-
        start}
    set parameter1 <value_str>

end
end
end

```

| Variable | Description | Default |
|--|--|----------|
| edit <layout name> | Enter the name of an existing layout or a new name. Press ? to view the list of existing layouts. | |
| title <text> | Enter a title for the current report layout. | |
| cache-time-out <seconds_int> | Enter the timeout period in seconds for cached datasets. Range 0 to 86 400. Default is 604 800 seconds (1 week). | 86400 |
| cutoff-option {run-time custom} | Select the end of the report period: run-time — the report period ends when the report is run. custom — the report period ends at cutoff-time. | run-time |
| cutoff-time <time_str> | Enter the end of the report period in hh:mm format. This field is available when cutoff-option is custom. | 00:00 |
| description <text> | Enter a description for the current layout. | |
| email-recipients <recipients_str> | Enter the email addresses of report recipients separated by semicolons. Available if email-send is enable. | Null |
| email-send {enable disable} | Enable or disable sending of reports by email. | disable |
| format {html pdf} | Select the layout format. | html |
| schedule-type {demand daily weekly} | Select the schedule type for the report layout. | daily |

| Variable | Description | Default |
|---|--|---------|
| time <HH:MM> | Enter the time for the report to be run. HH: Hour value in two digit format 0-23 MM: Minute value 0-59. schedule-type must be set in order for time option to be available. | 00:00 |
| day {sunday monday tuesday wednesday thursday friday saturday} | Select the day of the week for report to be run. day option is only available when schedule-type is set to weekly. | sunday |
| style-theme <theme name> | Enter the name of an existing style theme or a new style theme name. More detail on style themes can be found in theme section of this chapter. | |
| options {include-table-of-contents auto-numbering-heading view-chart-as-heading show-html-navbar-before-heading} | Use following options to configure the report page design; include-table-of-contents — select this option to include table of contents in the report. auto-numbering-heading — select this option to include page numbers in the heading. view-chart-as-heading — select this option to add heading for each chat automatically. show-html-navbar-before-heading — select this option to show html navigation bar before each heading. | |
| config page | | |
| paper{ A4 letter} | Select the standard paper size. | A4 |
| column-break-before {heading1 heading2 heading3} | Select the heading type which will include a column break in front of it. | |
| options {header-on-first-page footer-on-first-page} | Select one of these options to have the header or the footer on the first page of the report. | |
| config header | | |
| style <style name> | Enter the name of an existing style or a new name. Press ? to view the list of existing styles. | |
| config header-item | | |
| edit <item_id> | Enter the id of an existing report item or a new id. Press ? to view the list of existing report item ids. | |
| style <style name> | Enter the name of an existing style or a new name. Press ? to view the list of existing styles. | |
| type {text image} | Select the report header item type. | text |
| content <text> | Enter the content material for the header item. This option only available when type is set to text. | |
| description <text> | Enter the description of the image file. This option is only available when type is set to image. | |
| img-src <text> | Enter the name of the header item image file. For example image.jpg. This option is only available when type is set to image. | |

| Variable | Description | Default |
|---|--|---------|
| config footer | | |
| style <style name> | Enter the name of an existing style or a new name. Press ? to view the list of existing styles. | |
| config footer-item | | |
| edit <item_id> | Enter the id of an existing report item or a new id. Press ? to view the list of existing report item ids. | |
| style <style name> | Enter the name of an existing style or a new name. Press ? to view the list of existing styles. | |
| type {text image} | Select the report footer item type. | text |
| content <text> | Enter the content material for the footer item. This option only available when type is set to text. | |
| description <text> | Enter the description of the image file. This option is only available when type is set to image. | |
| img-src <text> | Enter the name of the footer item image file. For example image.jpg. This option is only available when type is set to image. | |
| config body-item | | |
| edit <item_id> | Enter the id of an existing report body item or a new id. Press ? to view the list of existing report body item ids. | |
| type {text image chart misc} | Select the body item type. | text |
| description <text> | Enter the content material for the body item. This option only available when type is set to text or misc. | |
| style <style name> | Enter the name of an existing style or a new name. Press ? to view the list of existing styles. | |
| text-component {heading1 heading2 heading3 normal text} | Select the text component type. | text |
| content <text> | Enter the content material for the text component. Headings are limited to only one line. | |
| img-src <text> | Enter the name of the body item image file. For example image.jpg. This option is only available when type is set to image. | |
| chart <chart name> | Enter the report item chart name. This option is only available when type is set to chart. | |
| chart-options {hide-title include-no-data show-caption} | Select one of the following options to customize the chart. hide-title: Hide chart title. include-no-data: Include the chart with no data. show-caption: Show chart caption. | |

| Variable | Description | Default |
|--|--|---------|
| misc-component {hline page-break column-break section- start} | Select one of the following options to add a separator component to your report. hline — add a horizontal line page-break — add a page break column-break — add a column break section-start — add a section | |
| parameter1 <value_str> | Enter the parameter value for this body item. | |

style

Use this command configure the report styles. Report styles help you configure font, paragraph and page properties of your reports. For example you can set the font type, size and color as well as page background color and page margins. You can select a style from a pre-defined list or you can create your own report style. Once you have all style parameters set, you can save it and use it on any reports. You can use the following options to customize or create report styles.

Syntax

```
config report style
edit <style name>
    set options {font | text | color | align | size | margin
                | border | padding | column}
    set font-family {Verdana | Arial | Helvetica | Courier | Times}
    set font-style {normal|italic}
    set font-weight {normal | bold}
    set font-size {xx-small | x-small | small | medium | large
                  | x-large | xx-large} | 5-28
    set line-height <integer | percentage>
    set fg-color {aqua | black | blue | fuchsia | gray | green
                  | lime | maroon | navy | olive | purple | red | silver
                  | teal | white | yellow | <color-value>}
    set bg-color {aqua | black | blue | fuchsia | gray | green
                  | lime | maroon | navy | olive | purple | red | silver
                  | teal | white | yellow | <color-value>}
    set align {left | center | right | justify}
    set height <integer | percentage>
    set width <integer | percentage>
    set margin-top <integer>
    set margin-bottom <integer>
    set margin-left <integer>
    set margin-right <integer>
    set border-top <topwidth_int> {none | dotted | dashed | solid}
                                {aqua | black | blue | fuchsia | gray | green | lime
                                | maroon | navy | olive | purple | red | silver | teal
                                | white | yellow | <color-value>}
    set border-bottom <bottomwidth_int> {none | dotted | dashed
                                         | solid} {aqua | black | blue | fuchsia | gray | green
                                         | lime | maroon | navy | olive | purple | red | silver
                                         | teal | white | yellow | <color-value>}
    set border-left <leftwidth_int> {none | dotted | dashed | solid}
                                {aqua | black | blue | fuchsia | gray | green | lime
                                | maroon | navy | olive | purple | red | silver | teal
                                | white | yellow | <color-value>}
    set border-right <rightwidth_int> {none | dotted | dashed
                                        | solid} {aqua | black | blue | fuchsia | gray | green
                                        | lime | maroon | navy | olive | purple | red | silver
                                        | teal | white | yellow | <color-value>}
```

```

set padding-top <integer>
set padding-bottom <integer>
set padding-left <integer>
set padding-right <integer>
set column-span {none|all}
set column-gap <integer>
end

```

| Variable | Description | Default |
|--|---|---------|
| edit <style name> | Enter the name of an existing style or a new name. Press ? to view the list of existing styles. | |
| options {font text color align size margin border padding column} | Select report style feature for customization. For example, set font allows you to customize font properties. | |
| font-family {Verdana Arial Helvetica Courier Times} | Select one of the pre-defined font families for the current report style. | |
| font-style {normal italic} | Select the style of the font. | normal |
| font-weight {normal bold} | Select the weight of the font. | normal |
| font-size {xx-small x-small small medium large x-large xx-large} 5-28 | Select one of the pre-defined font size options or enter a number between 5 and 28 which sets the font size in pixels. | |
| line-height <integer percentage> | Set the line height in pixels or percentage. For example 10 or 120%. | |
| fg-color {aqua black blue fuchsia gray green lime maroon navy olive purple red silver teal white yellow <color-value>} | Select the foreground color from one of the pre-defined colors or enter 6 digit hex color code. For example 0033CC is for blue. | |
| bg-color {aqua black blue fuchsia gray green lime maroon navy olive purple red silver teal white yellow <color-value>} | Select the background color from one of the pre-defined colors or enter 6 digit hex color code. For example FF0000 is for red. | |
| align {left center right justify} | Select one of the text alignment options. | left |
| height <integer percentage> | Enter the height of the report in pixels or percentage. For example 10 or 120%. | |
| width <integer percentage> | Enter the height of the report in pixels or percentage. For example 10 or 120%. | |
| margin-top <integer> | Enter the top margin size in pixels. | |

| Variable | Description | Default |
|--|---|---------|
| margin-bottom <integer> | Enter the bottom margin size in pixels. | |
| margin-left <integer> | Enter the left margin size in pixels. | |
| margin-right <integer> | Enter the right margin size in pixels. | |
| border-top <topwidth_int> { none dotted dashed solid } { aqua black blue fuchsia gray green lime maroon navy olive purple red silver teal white yellow <color-value> } | Enter the top border width in pixels followed by the border style and the border color. Border color can be entered by name or 6 digit hex color code. | none |
| border-bottom <bottomwidth_int> { none dotted dashed solid } { aqua black blue fuchsia gray green lime maroon navy olive purple red silver teal white yellow <color-value> } | Enter the bottom border width in pixels followed by the border style and the border color. Border color can be entered by name or 6 digit hex color code. | none |
| border-left <leftwidth_int> { none dotted dashed solid } { aqua black blue fuchsia gray green lime maroon navy olive purple red silver teal white yellow <color-value> } | Enter the left border width in pixels followed by the border style and the border color. Border color can be entered by name or 6 digit hex color code. | none |
| border-right <rightwidth_int> { none dotted dashed solid } { aqua black blue fuchsia gray green lime maroon navy olive purple red silver teal white yellow <color-value> } | Enter the right border width in pixels followed by the border style and the border color. Border color can be entered by name or 6 digit hex color code. | none |
| padding-top <integer> | Enter the top padding size in pixels. | |
| padding-bottom <integer> | Enter the bottom padding size in pixels. | |

| Variable | Description | Default |
|----------------------------|--|---------|
| padding-left <integer> | Enter the left padding size in pixels. | |
| padding-right <integer> | Enter the right padding size in pixels. | |
| column-span {none all} | Select <code>all</code> for span across all columns or <code>none</code> for no span | none |
| column-gap <integer> | Enter the column gap size in pixels. | |

summary

Use this command to add widgets (also called charts) to the Executive Summary and to configure the schedule for updating the data displayed by the widget. The data is updated by executing the SQL query in the widget and refreshing the information displayed in the widget.

Syntax

```
config report summary
  edit id <integer>
    set column {1 | 2}
    set day {sunday | monday | tuesday | wednesday | thursday
           | friday | saturday}
    set schedule {daily | weekly}
    set time <hh:mm>
    set widget <widget_name>
  end
```

| Variable | Description | Default |
|--|--|---------|
| id <integer> | Enter the identification number for the log field. | |
| column {1 2} | Select the column of the Executive Summary to display the widget in. | 1 |
| day {sunday monday tuesday wednesday thursday friday saturday} | Set the day of the week to update the widget. Available if schedule is weekly. | sunday |
| schedule {daily weekly} | Schedule the widget to update once a day or once a week. | daily |
| time <hh:mm> | Set the time of day to update the widget. You can set the time of day for weekly or daily updates. | 00:00 |
| widget <widget_name> | Select the name of the widget. | |

theme

Use this command configure themes for your reports. Themes help you configure some of the main characteristics of your report outlook. For example you can configure the page orientation of the report or create sub-styles for title headings. You can select a theme from a pre-defined list or you can create your own report theme. Once you have all theme parameters set, you can save it and use it on any reports. You can use the following options to customize or create report themes.

Syntax

```
config report theme
  edit <theme name>
    set page-orient {portrait | landscape}
    set column-count {1 | 2 | 3}
    set default-html-style <style_name>
    set default-pdf-style <style_name>
    set page-style <style_name>
    set page-header-style <style_name>
    set page-footer-style <style_name>
    set report-title-style <style_name>
    set report-subtitle-style <style_name>
    set heading1-style <style_name>
    set heading2-style <style_name>
    set heading3-style <style_name>
    set heading4-style <style_name>
    set toc-title-style <style_name>
    set toc-heading1-style <style_name>
    set toc-heading2-style <style_name>
    set toc-heading3-style <style_name>
    set toc-heading4-style <style_name>
    set normal-text-style <style_name>
    set bullet-text-style <style_name>
    set numbered-text-style <style_name>
    set image-style <style_name>
    set hline-style <style_name>
    set graph-chart-style <style_name>
    set table-chart-style <style_name>
    set table-chart-caption-style <style_name>
    set table-chart-head-style <style_name>
    set table-chart-odd-row-style <style_name>
    set table-chart-even-row-style <style_name>
  end
```

| Variable | Description | Default |
|---------------------------------------|---|----------|
| edit <theme name> | Enter the name of an existing theme or a new name. Press ? to view the list of existing themes. | |
| page-orient {portrait landscape} | Select the page orientation for the current report theme. | portrait |

| Variable | Description | Default |
|---------------------------------------|--|---------|
| column-count { 1 2 3 } | Enter the number of columns for the current report theme. The maximum value is 3. | 1 |
| default-html-style <style_name> | Enter the default html style name. Press ? to view the list of existing html styles. | |
| default-pdf-style <style_name> | Enter the default pdf style name. Press ? to view the list of existing pdf styles. | |
| page-style <style_name> | Enter the default page style name. Press ? to view the list of existing page styles. | |
| page-header-style <style_name> | Enter the default page header style name. Press ? to view the list of existing page header styles. | |
| page-footer-style <style_name> | Enter the default footer style name. Press ? to view the list of existing footer styles. | |
| report-title-style <style_name> | Enter the default report title style name. Press ? to view the list of existing report title styles. | |
| report-subtitle-style <style_name> | Enter the default report subtitle style name. Press ? to view the list of existing report subtitle styles. | |
| heading1-style <style_name> | Enter the default heading1 style name. Press ? to view the list of existing heading1 styles. | |
| heading2-style <style_name> | Enter the default heading2 style name. Press ? to view the list of existing heading2 styles. | |
| heading3-style <style_name> | Enter the default heading3 style name. Press ? to view the list of existing heading3 styles. | |
| heading4-style <style_name> | Enter the default html style name. Press ? to view the list of existing html styles. | |
| toc-title-style <style_name> | Enter the default table of contents style name. Press ? to view the list of existing table of contents styles. | |
| toc-heading1-style <style_name> | Enter the default table of contents heading1 style name. Press ? to view the list of existing table of contents heading1 styles. | |
| toc-heading2-style <style_name> | Enter the default table of contents heading2 style name. Press ? to view the list of existing table of contents heading2 styles. | |
| toc-heading3-style <style_name> | Enter the default table of contents heading3 style name. Press ? to view the list of existing table of contents heading3 styles. | |
| toc-heading4-style <style_name> | Enter the default table of contents heading4 style name. Press ? to view the list of existing table of contents heading4 styles. | |
| normal-text-style <style_name> | Enter the default normal text style name. Press ? to view the list of existing normal text styles. | |
| bullet-text-style <style_name> | Enter the default bullet text style name. Press ? to view the list of existing bullet text styles. | |
| numbered-text-style <style_name> | Enter the default numbered text style name. Press ? to view the list of existing numbered text styles. | |
| image-style <style_name> | Enter the default image style name. Press ? to view the list of existing image styles. | |
| hline-style <style_name> | Enter the default horizontal line style name. Press ? to view the list of existing horizontal line styles. | |

| Variable | Description | Default |
|--|--|---------|
| graph-chart-style <style_name> | Enter the default graph chart style name. Press ? to view the list of existing graph chart styles. | |
| table-chart-style <style_name> | Enter the default table chart style name. Press ? to view the list of existing table chart styles. | |
| table-chart-caption-style <style_name> | Enter the default table chart caption style name. Press ? to view the list of existing table chart caption styles. | |
| table-chart-head-style <style_name> | Enter the default table chart header style name. Press ? to view the list of existing table chart header styles. | |
| table-chart-odd-row-style <style_name> | Enter the default table chart odd row style name. Press ? to view the list of existing table chart odd row styles. | |
| table-chart-even-row-style <style_name> | Enter the default table chart even row style name. Press ? to view the list of existing table chart even row styles. | |

router

Routers move packets from one network segment to another towards a network destination. When a packet reaches a router, the router uses data in the packet header to look up a suitable route on which to forward the packet to the next segment. The information that a router uses to make routing decisions is stored in a routing table. Other factors related to the availability of routes and the status of the network may influence the route selection that a router makes when forwarding a packet to the next segment.

The FortiGate unit supports many advanced routing functions and is compatible with industry standard Internet routers. The FortiGate unit can communicate with other routers to determine the best route for a packet.

The following `router` commands are available to configure options related to FortiGate unit router communications and packet forwarding:

| | | |
|---|---|---------------------------|
| access-list, access-list6 | key-chain | rip |
| aspath-list | multicast | ripng |
| auth-path | multicast6 | route-map |
| bfd | multicast-flow | setting |
| bgp | ospf | static |
| community-list | ospf6 | static6 |
| gwdetect | policy, policy6 | |
| isis | prefix-list, prefix-list6 | |

access-list, access-list6

Use this command to add, edit, or delete access lists. Access lists are filters used by FortiGate unit routing processes. For an access list to take effect, it must be called by a FortiGate unit routing process (for example, a process that supports RIP or OSPF). Use `access-list6` for IPv6 routing.

Each rule in an access list consists of a prefix (IP address and netmask), the action to take for this prefix (permit or deny), and whether to match the prefix exactly or to match the prefix and any more specific prefix.



If you are setting a prefix of 128.0.0.0, use the format 128.0.0.0/1. The default route, 0.0.0.0/0 can not be exactly matched with an access-list. A prefix-list must be used for this purpose. For more information, see [“router prefix-list, prefix-list6” on page 421](#).

The FortiGate unit attempts to match a packet against the rules in an access list starting at the top of the list. If it finds a match for the prefix, it takes the action specified for that prefix. If no match is found the default action is deny.

Syntax

```
config router access-list, access-list6
  edit <access_list_name>
    set comments <string>
    config rule
      edit <access_list_id>
        set action {deny | permit}
        set exact-match {enable | disable}
        set prefix { <prefix_ipv4mask> | any }
        set prefix6 { <prefix_ipv6mask> | any }
        set wildcard <address_ipv4> <wildcard_mask>
      end
    end
  end
```



The action and prefix fields are required. The exact-match field is optional.

| Variable | Description | Default |
|------------------------------|---|-------------|
| edit <access_list_name> | Enter a name for the access list. An access list and a prefix list cannot have the same name. | No default. |
| comments <string> | Enter a descriptive comment. The max length is 127 characters. | No default. |
| config rule variables | | |
| edit <access_list_id> | Enter an entry number for the rule. The number must be an integer. | No default. |
| action {deny permit} | Set the action to take for this prefix. | permit |

| Variable | Description | Default |
|---|---|-------------|
| exact-match { enable disable } | By default, access list rules are matched on the prefix or any more specific prefix. Enable <code>exact-match</code> to match only the configured prefix. | disable |
| prefix { <prefix_ipv4mask> any } | Enter the prefix for this access list rule. Enter either: <ul style="list-style-type: none"> IPv4 address and network mask any — match any prefix. | any |
| prefix6 { <prefix_ipv6mask> any } | Enter the prefix for this IPv6 access list rule. Enter either: <ul style="list-style-type: none"> IPv6 address and network mask any — match any prefix. <p>This variable is only used with <code>config access-list6</code>.</p> | any |
| wildcard <address_ipv4> <wildcard_mask> | Enter the IP address and reverse (wildcard) mask to process. The value of the mask (for example, 0.0.255.0) determines which address bits to match. A value of 0 means that an exact match is required, while a binary value of 1 indicates that part of the binary network address does not have to match. You can specify discontinuous masks (for example, to process “even” or “odd” networks according to any network address octet). For best results, do not specify a <code>wildcard</code> attribute unless <code>prefix</code> is set to <code>any</code> . This variable is only used with <code>config access-list</code> . | No default. |

aspath-list

Use this command to set or unset BGP AS-path list parameters. By default, BGP uses an ordered list of Autonomous System (AS) numbers to describe the route that a packet takes to reach its destination. A list of these AS numbers is called the AS path. You can filter BGP routes using AS path lists.

When the FortiGate unit receives routing updates from other autonomous systems, it can perform operations on updates from neighbors and choose the shortest path to a destination. The shortest path is determined by counting the AS numbers in the AS path. The path that has the least AS numbers is considered the shortest AS path.

Use the `config router aspath-list` command to define an access list that examines the AS_PATH attributes of BGP routes to match routes. Each entry in the AS-path list defines a rule for matching and selecting routes based on the setting of the AS_PATH attribute. The default rule in an AS path list (which the FortiGate unit applies last) denies the matching of all routes.

Syntax

```
config router aspath-list
  edit <aspath_list_name>
    config rule
      edit <as_rule_id>
        set action {deny | permit}
        set regexp <regexp_str>
      end
    end
  end
```



The `action` and `regexp` fields are required.

| Variable | Description | Default |
|----------------------------|--|-------------|
| edit <aspath_list_name> | Enter a name for the AS path list. | No default. |
| config rule variables | | |
| edit <as_rule_id> | Enter an entry number for the rule. The number must be an integer. | No default. |
| action {deny permit} | Deny or permit operations on a route based on the value of the route's AS_PATH attribute. | No default. |
| regexp <regexp_str> | Specify the regular expression that will be compared to the AS_PATH attribute (for example, ^730\$). The value is used to match AS numbers. Delimit a complex <code>regexp_str</code> value using double-quotation marks. | Null |

auth-path

Authentication based routing allows firewall policies to direct network traffic flows. This command configures a RADIUS object on your FortiGate unit. The same object is required to be configured on the RADIUS server.

To configure authentication based routing on your FortiGate unit

- 1. Configure your FortiGate unit to communicate with a RADIUS authentication server.
- 2. Configure a user that uses the RADIUS server.
- 3. Add that user to a user group configured to use the RADIUS server.
- 4. Configure the router auth-path object.
- 5. Configure a custom service for RADIUS traffic.
- 6. Configure a service group that includes RADIUS traffic along with other types of traffic that will be allowed to pass through the firewall.
- 7. Configure a firewall policy that has route based authentication enabled.

The Fortinet Knowledge Base has an article on authentication based routing that provides a sample configuration for these steps.



The auth-path command is not available when the FortiGate unit is in Transparent mode.

Syntax

```
config router auth-path
  edit <aspath_list_name>
    set device <interface>
    set gateway <gway_ipv4>
  end
```

| Variable | Description | Default |
|-----------------------|---|-------------|
| edit <auth_path_name> | Enter a name for the authentication path. | No default. |
| device <interface> | Specify the interface for this path. | No default. |
| gateway <gway_ipv4> | Specify the gateway IP address for this path. | Null. |

bfd

Use this command to enable Bidirectional Forwarding Detection (BFD) when there is no dynamic routing active.

Syntax

```
config router bfd
  config neighbor
    edit <neighbor_IPv4_addr>
      set interface <if_name>
    next
  end
end
```

| Variable | Description | Default |
|----------------------|---|---------|
| <neighbor_IPv4_addr> | Enter the neighbor's IP address. | 0.0.0.0 |
| interface <if_name> | Enter the name of the interface to monitor. | None. |

bgp

Use this command to set or unset BGP-4 routing parameters. BGP can be used to perform Classless Interdomain Routing (CIDR) and to route traffic between different autonomous systems or domains using an alternative route if a link between a FortiGate unit and a BGP peer (such as an ISP router) fails. FortiOS BGP4 complies with RFC 1771 and supports IPv4 addressing.

FortiOS supports IPv6 over BGP4 via the BGP4+ protocol defined in RFC 2545, and RFC 2858. IPv6 configuration for BGP is accomplished with the `aggregate-address6`, `network6`, and `redistribute6` variables. Also almost every variable in `config neighbour` has an IPv4 and IPv6 version such as `activate` and `activate6`. Any variable ending with a “6” is an IPv6 variable.

When BGP is enabled, the FortiGate unit sends routing table updates to the upstream ISP router whenever any part of the routing table changes. The update advertises which routes can be used to reach the FortiGate unit. In this way, routes are made known from the border of the internal network outwards (routes are pushed forward) instead of relying on upstream routers to propagate alternative paths to the FortiGate unit.

FortiGate unit BGP supports the following extensions to help manage large numbers of BGP peers:

- **Communities** — The FortiGate unit can set the COMMUNITY attribute of a route to assign the route to predefined paths (see RFC 1997). The FortiGate unit can examine the COMMUNITY attribute of learned routes to perform local filtering and/or redistribution.
- **Internal BGP (IBGP) route reflectors** — The FortiGate unit can operate as a route reflector or participate as a client in a cluster of IBGP peers (see RFC 1966).
- **External BGP (EBGP) confederations** — The FortiGate unit can operate as a confederation member, using its AS confederation identifier in all transactions with peers that are not members of its confederation (see RFC 3065).

Bi-directional Forwarding Detection (BFD) is a protocol used by BGP, and OSPF. It is used to quickly locate hardware failures in the network. Routers running BFD send unicast messages to each other, and if a timer runs out, meaning no messages have been received, on a connection then that unresponsive router is declared down. BFD then communicates this information to the routing protocol and the routing information is updated. BFD support can only be configured through the CLI.

Syntax

```
config router bgp
    set always-compare-med {enable | disable}
    set as <local_as_id>
    set bestpath-as-path-ignore {enable | disable}
    set bestpath-cmp-confed-aspath {enable | disable}
    set bestpath-cmp-routerid {enable | disable}
    set bestpath-med-confed {enable | disable}
    set bestpath-med-missing-as-worst {enable | disable}
    set client-to-client-reflection {enable | disable}
    set cluster-id <address_ipv4>
    set confederation-identifier <peerid_integer>
    set dampening {enable | disable}
    set dampening-max-suppress-time <minutes_integer>
    set dampening-reachability-half-life <minutes_integer>
    set dampening-reuse <reuse_integer>
```

```
set dampening-route-map <routemap-name_str>
set dampening-suppress <limit_integer>
set dampening-unreachability-half-life <minutes_integer>
set default-local-preference <preference_integer>
set deterministic-med {enable | disable}
set distance-external <distance_integer>
set distance-internal <distance_integer>
set distance-local <distance_integer>
set ebgp-multipath {enable | disable}
set enforce-first-as {disable | enable}
set fast-external-failover {disable | enable}
set graceful-restart {disable | enable}
set graceful-restart-time <restart_time>
set graceful-stalepath-time <stalepath_time>
set graceful-update-delay <delay_time>
set holdtime-timer <seconds_integer>
set ibgp-multipath {enable | disable}
set ignore_optional_capability {disable | enable}
set keepalive-timer <seconds_integer>
set log-neighbor-changes {disable | enable}
set network-import-check {disable | enable}
set router-id <address_ipv4>
set scan-time <seconds_integer>
set synchronization {enable | disable}
config admin-distance
    edit <route_entry_id>
        set distance <integer>
        set neighbor-prefix <ip_and_netmask>
        set route-list <string>
    end
config aggregate-address, config aggregate-address6
    edit <aggr_addr_id>
        set as-set {enable | disable}
        set prefix <address_ipv4mask>
        set summary-only {enable | disable}
    end
config aggregate-address, config aggregate-address6
    edit <aggr_addr_id>
        set as-set {enable | disable}
        set prefix6 <address_ipv6mask>
        set summary-only {enable | disable}
    end
```

```
config neighbor
edit <neighbor_address_ipv4>
    set activate {enable | disable}
    set activate6 {enable | disable}
    set advertisement-interval <seconds_integer>
    set allowas-in <max_num_AS_integer>
    set allowas-in6 <max_num_AS_integer>
    set allowas-in-enable {enable | disable}
    set allowas-in-enable6 {enable | disable}
    set as-override {enable | disable}
    set as-override6 {enable | disable}
    set attribute-unchanged [as-path] [med] [next-hop]
    set attribute-unchanged6 [as-path] [med] [next-hop]
    set bfd {enable | disable}
    set capability-default-originate {enable | disable}
    set capability-default-originate6 {enable | disable}
    set capability-dynamic {enable | disable}
    set capability-graceful-restart {enable | disable}
    set capability-graceful-restart6 {enable | disable}
    set capability-orf {both | none | receive | send}
    set capability-orf6 {both | none | receive | send}
    set capability-route-refresh {enable | disable}
    set connect-timer <seconds_integer>
    set default-originate-routemap <routemap_str>
    set default-originate-routemap6 <routemap_str>
    set description <text_str>
    set distribute-list-in <access-list-name_str>
    set distribute-list-in6 <access-list-name_str>
    set distribute-list-out <access-list-name_str>
    set distribute-list-out6 <access-list-name_str>
    set dont-capability-negotiate {enable | disable}
    set ebgp-enforce-multihop {enable | disable}
    set ebgp-multihop-ttl <seconds_integer>
    set filter-list-in <aspath-list-name_str>
    set filter-list-in6 <aspath-list-name_str>
    set filter-list-out <aspath-list-name_str>
    set filter-list-out6 <aspath-list-name_str>
    set holdtime-timer <seconds_integer>
    set interface <interface-name_str>
    set keep-alive-timer <seconds_integer>
    set maximum-prefix <prefix_integer>
    set maximum-prefix6 <prefix_integer>
    set maximum-prefix-threshold <percentage_integer>
    set maximum-prefix-threshold6 <percentage_integer>
    set maximum-prefix-warning-only {enable | disable}
    set maximum-prefix-warning-only6 {enable | disable}
    set next-hop-self {enable | disable}
    set next-hop-self6 {enable | disable}
    set override-capability {enable | disable}
```

```
set passive {enable | disable}
set password <string>
set prefix-list-in <prefix-list-name_str>
set prefix-list-in6 <prefix-list-name_str>
set prefix-list-out <prefix-list-name_str>
set prefix-list-out6 <prefix-list-name_str>
set remote-as <id_integer>
set remove-private-as {enable | disable}
set remove-private-as6 {enable | disable}
set retain-stale-time <seconds_integer>
set route-map-in <routemap-name_str>
set route-map-in6 <routemap-name_str>
set route-map-out <routemap-name_str>
set route-map-out6 <routemap-name_str>
set route-reflector-client {enable | disable}
set route-reflector-client6 {enable | disable}
set route-server-client {enable | disable}
set route-server-client6 {enable | disable}
set send-community {both | disable | extended | standard}
set send-community6 {both | disable | extended | standard}
set shutdown {enable | disable}
set soft-reconfiguration {enable | disable}
set strict-capability-match {enable | disable}
set unsuppress-map <route-map-name_str>
set update-source <interface-name_str>
set weight <weight_integer>
end
config network, config network6
edit <network_id>
set backdoor {enable | disable}
set prefix <address_ipv4mask>
set route-map <routemap-name_str>
end
config network, config network6
edit <network_id>
set backdoor {enable | disable}
set prefix6 <address_ipv6mask>
set route-map <routemap-name_str>
end
config redistribute, config redistribute6 {connected | static |
rip | ospf}
set status {enable | disable}
set route-map <route-map-name_str>
end
config redistribute, config redistribute6 {connected | static |
rip | ospf}
set status {enable | disable}
set route-map <route-map-name_str>
end
```

config router bgp

Use this command to enable a Border Gateway Protocol version 4 (BGP-4) process on the FortiGate unit, define the interfaces making up the local BGP network (see the subcommand [“config network, config network6” on page 365](#)), and set operating parameters for communicating with BGP neighbors (see the subcommand [“config neighbor” on page 356](#)).

When multiple routes to the FortiGate unit exist, BGP attributes determine the best route and the FortiGate unit communicates this information to its BGP peers. The best route is added to the IP routing table of the BGP peer, which in turn propagates this updated routing information to upstream routers.

FortiGate units maintain separate entries in their routing tables for BGP routes. See [“Using route maps with BGP” on page 440](#). To reduce the size of the BGP routing table and conserve network resources, you can optionally aggregate routes to the FortiGate unit. An aggregate route enables the FortiGate unit to advertise one block of contiguous IP addresses as a single, less-specific address. You can implement aggregate routing either by redistributing an aggregate route (see the subcommand [“config redistribute, config redistribute6” on page 366](#)) or by using the conditional aggregate routing feature (see the subcommand [“config aggregate-address, config aggregate-address6” on page 355](#)).



In the following table, the `as` and `router-id` fields are required. All other fields are optional.

| Variable | Description | Default |
|---|--|---------|
| <code>always-compare-med</code> {enable disable} | Enable or disable the comparison of MULTI_EXIT_DISC (Multi Exit Discriminator or MED) attributes for identical destinations advertised by BGP peers in different autonomous systems. | disable |
| <code>as <local_as_id></code> | Enter an integer to specify the local autonomous system (AS) number of the FortiGate unit. The range is from 1 to 4 294 967 295. A value of 0 disables BGP. When the <code>local_as_id</code> number is different than the AS number of the specified BGP neighbor (see “remote-as <id_integer>” on page 362), an External BGP (EBGP) session is started. Otherwise, an Internal BGP (IBGP) session is started. | 0 |
| <code>bestpath-as-path-ignore</code> {enable disable} | Enable or disable the inclusion of an AS path in the selection algorithm for choosing a BGP route. | disable |
| <code>bestpath-cmp-confed-aspath</code> {enable disable} | Enable or disable the comparison of the AS_CONFED_SEQUENCE attribute, which defines an ordered list of AS numbers representing a path from the FortiGate unit through autonomous systems within the local confederation. | disable |
| <code>bestpath-cmp-routerid</code> {enable disable} | Enable or disable the comparison of the router-ID values for identical EBGP paths. | disable |
| <code>bestpath-med-confed</code> {enable disable} | Enable or disable the comparison of MED attributes for routes advertised by confederation EBGP peers. | disable |

| Variable | Description | Default |
|--|---|---------|
| bestpath-med-missing-as-worst {enable disable} | This field is available when <code>bestpath-med-confed</code> is set to <code>enable</code> . When <code>bestpath-med-confed</code> is enabled, treat any confederation path with a missing MED metric as the least preferred path. | disable |
| client-to-client-reflection {enable disable} | Enable or disable client-to-client route reflection between IBGP peers. If the clients are fully meshed, route reflection may be disabled. | enable |
| cluster-id <address_ipv4> | Set the identifier of the route-reflector in the cluster ID to which the FortiGate unit belongs. If 0 is specified, the FortiGate unit operates as the route reflector and its <code>router-id</code> value is used as the <code>cluster-id</code> value. If the FortiGate unit identifies its own cluster ID in the CLUSTER_LIST attribute of a received route, the route is ignored to prevent looping. | 0.0.0.0 |
| confederation-identifier <peerid_integer> | Set the identifier of the confederation to which the FortiGate unit belongs. The range is from 1 to 65 535. | 0 |
| dampening {enable disable} | Enable or disable route-flap dampening on all BGP routes. See RFC 2439. (A flapping route is unstable and continually transitions down and up.) If you set dampening, you may optionally set <code>dampening-route-map</code> or define the associated values individually using the <code>dampening-*</code> fields. | disable |
| dampening-max-suppress-time <minutes_integer> | This field is available when <code>dampening</code> is set to <code>enable</code> . Set the maximum time (in minutes) that a route can be suppressed. The range is from 1 to 255. A route may continue to accumulate penalties while it is suppressed. However, the route cannot be suppressed longer than <code>minutes_integer</code> . | 60 |
| dampening-reachability-half-life <minutes_integer> | This field is available when <code>dampening</code> is set to <code>enable</code> . Set the time (in minutes) after which any penalty assigned to a reachable (but flapping) route is decreased by half. The range is from 1 to 45. | 15 |
| dampening-reuse <reuse_integer> | This field is available when <code>dampening</code> is set to <code>enable</code> . Set a dampening-reuse limit based on accumulated penalties. The range is from 1 to 20 000. If the penalty assigned to a flapping route decreases enough to fall below the specified <code>reuse_integer</code> , the route is not suppressed. | 750 |
| dampening-route-map <routermap_name_str> | This field is available when <code>dampening</code> is set to <code>enable</code> . Specify the route-map that contains criteria for dampening. You must create the route-map before it can be selected here. See “route-map” on page 438 and “Using route maps with BGP” on page 440 . | Null. |
| dampening-suppress <limit_integer> | This field is available when <code>dampening</code> is set to <code>enable</code> . Set a dampening-suppression limit. The range is from 1 to 20 000. A route is suppressed (not advertised) when its penalty exceeds the specified limit. | 2 000 |

| Variable | Description | Default |
|--|--|---------|
| dampening-unreachability-half-life <minutes_integer> | This field is available when dampening is set to enable. Set the time (in minutes) after which the penalty on a route that is considered unreachable is decreased by half. The range is from 1 to 45. | 15 |
| default-local-preference <preference_integer> | Set the default local preference value. A higher value signifies a preferred route. The range is from 0 to 4 294 967 295. | 100 |
| deterministic-med {enable disable} | Enable or disable deterministic comparison of the MED attributes of routes advertised by peers in the same AS. | disable |
| distance-external <distance_integer> | Set the administrative distance of EBGp routes. The range is from 1 to 255. If you set this value, you must also set values for distance-internal and distance-local. | 20 |
| distance-internal <distance_integer> | This field is available when distance-external is set. Set the administrative distance of IBGP routes. The range is from 1 to 255. | 200 |
| distance-local <distance_integer> | This field is available when distance-external is set. Set the administrative distance of local BGP routes. The range is from 1 to 255. | 200 |
| ebgp-multipath {enable disable} | Enable or disable ECMP load balancing across multiple (four) eBGP connections. | disable |
| enforce-first-as {disable enable} | Enable or disable the addition of routes learned from an EBGp peer when the AS number at the beginning of the route's AS_PATH attribute does not match the AS number of the EBGp peer. | disable |
| fast-external-failover {disable enable} | Immediately reset the session information associated with BGP external peers if the link used to reach them goes down. | enable |
| graceful-restart {disable enable} | Enable or disable BGP support for the graceful restart feature. Graceful restart limits the effects of software problems by allowing forwarding to continue when the control plane of the router fails. It also reduces routing flaps by stabilizing the network. | disable |
| graceful-restart-time <restart_time> | Set the time in seconds needed for neighbors to restart after a graceful restart. The range is 1 to 3600 seconds. Available when graceful-restart is enabled. | 120 |
| graceful-stalepath-time <stalepath_time> | Set the time in seconds to hold stale paths of restarting neighbors. The range is 1 to 3600 seconds. Available when graceful-restart is enabled. | 360 |
| graceful-update-delay <delay_time> | Route advertisement and selection delay in seconds after a graceful restart. The range is 1 to 3600 seconds. Available when graceful-restart is enabled. | 120 |
| holdtime-timer <seconds_integer> | The maximum amount of time in seconds that may expire before the FortiGate unit declares any BGP peer down. A keepalive message must be received every seconds_integer seconds, or the peer is declared down. The value can be 0 or an integer in the 3 to 65 535 range. | 180 |

| Variable | Description | Default |
|--|---|---------|
| ibgp-multipath {enable disable} | Enable or disable ECMP load balancing across multiple (four) iBGP connections. | disable |
| ignore_optional_capability {disable enable} | Don't send unknown optional capability notification message. | disable |
| keepalive-timer <seconds_integer> | The frequency (in seconds) that a keepalive message is sent from the FortiGate unit to any BGP peer. The range is from 0 to 65 535. BGP peers exchange keepalive messages to maintain the connection for the duration of the session. | 60 |
| log-neighbor-changes {disable enable} | Enable or disable the logging of changes to BGP neighbor status. | disable |
| network-import-check {disable enable} | Enable or disable the advertising of the BGP network in IGP (see the subcommand “ config network, config network6 ” on page 365). | enable |
| router-id <address_ipv4> | Specify a fixed identifier for the FortiGate unit. A value of 0.0.0.0 is not allowed. If router-id is not explicitly set, the highest IP address of the VDOM will be used as the default router-id. | 0.0.0.0 |
| scan-time <seconds_integer> | Configure the background scanner interval (in seconds) for next-hop route scanning. The range is from 5 to 60. | 60 |
| synchronization {enable disable} | Only advertise routes from iBGP if routes are present in an interior gateway protocol (IGP) such as RIP or OSPF. | disable |

Example

The following example defines the number of the AS of which the FortiGate unit is a member. It also defines an EBGP neighbor at IP address 10.0.1.2.

```
config router bgp
    set as 65001
    set router-id 172.16.120.20
    config neighbor
        edit 10.0.1.2
            set remote-as 65100
        end
    end
```

config admin-distance

Use this subcommand to set administrative distance modifications for bgp routes.

| Variable | Description | Default |
|--------------------------|---|-------------|
| edit <route_entry_id> | Enter an ID number for the entry. The number must be an integer. | No default. |
| distance <integer> | The administrative distance to apply to the route. This value can be from 1 to 255. | No default. |

| Variable | Description | Default |
|-------------------------------------|--|-------------|
| neighbor-prefix <ip_and_netmask> | Neighbor address prefix. This variable must be a valid IP address and netmask. | No default. |
| route-list <string> | The list of routes this distance will be applied to. The routes in this list can only come from the access-list which can be viewed at <code>config router access-list</code> . | No default. |

Example

This example shows how to manually adjust the distance associated with a route. It shows adding 25 to the weight of the route, that it will apply to neighbor routes with an IP address of 192.168.0.0 and a netmask of 255.255.0.0, that are also permitted by the access-list “downtown_office”.

```
config router bgp
  config admin-distance
    edit 1
      set distance 25
      set neighbour-prefix 192.168.0.0 255.255.0.0
      set route-list downtown_office
    next
  end
end
```

config aggregate-address, config aggregate-address6

Use this subcommand to set or unset BGP aggregate-address table parameters. The subcommand creates a BGP aggregate entry in the FortiGate unit routing table. Use `config aggregate-address6` for IPv6 routing.

When you aggregate routes, routing becomes less precise because path details are not readily available for routing purposes. The aggregate address represents addresses in several autonomous systems. Aggregation reduces the length of the network mask until it masks only the bits that are common to all of the addresses being summarized.



The `prefix` field is required. All other fields are optional.

| Variable | Description | Default |
|------------------------------|---|--------------------|
| edit <aggr_addr_id> | Enter an ID number for the entry. The number must be an integer. | No default. |
| as-set {enable disable} | Enable or disable the generation of an unordered list of AS numbers to include in the path information. When <code>as-set</code> is enabled, a <code>set-atomic-aggregate</code> value (see “Using route maps with BGP” on page 440) does not have to be specified. | disable |
| prefix <address_ipv4mask> | Set an aggregate prefix. Include the IP address and netmask. | 0.0.0.0 0.0.0.0 |

| Variable | Description | Default |
|------------------------------------|--|---------|
| prefix6 <address_ipv6mask> | Set an aggregate IPv6 prefix. Include the IP address and netmask. | ::/0 |
| summary-only {enable disable} | Enable or disable the advertising of aggregate routes only (the advertising of specific routes is suppressed). | disable |

Example

This example shows how to define an aggregate prefix of 192.168.0.0/16. The `as-set` command enables the generation of an unordered list of AS numbers to include in the path information.

```
config router bgp
  config aggregate-address
    edit 1
      set prefix 192.168.0.0/16
      set as-set enable
    end
  end
```

config neighbor

Use this subcommand to set or unset BGP neighbor configuration settings. The subcommand adds a BGP neighbor configuration to the FortiGate unit.

You can add up to 1000 BGP neighbors, and optionally use MD5 authentication to password protect BGP sessions with those neighbors. (see RFC 2385)

You can clear all or some BGP neighbor connections (sessions) using the `execute router clear bgp` command (see [“execute router clear bgp” on page 978](#)).



The `remote-as` field is required. All other fields are optional.

| Variable | Description | Default |
|---|--|-------------|
| edit <neighbor_address_ipv4> | Enter the IP address of the BGP neighbor. You can have up to 1000 configured neighbors. | No default. |
| activate {enable disable} | Enable or disable the address family for the BGP neighbor. | enable |
| activate6 {enable disable} | Enable or disable the address family for the BGP neighbor (IPv6). | enable |
| advertisement-interval <seconds_integer> | Set the minimum amount of time (in seconds) that the FortiGate unit waits before sending a BGP routing update to the BGP neighbor. The range is from 0 to 600. | 30 |

| Variable | Description | Default |
|--|--|------------|
| <code>allowas-in</code> <max_num_AS_integer> | <p>This field is available when <code>allowas-in-enable</code> is set to <code>enable</code>.</p> <p>Set the maximum number of occurrences your AS number is allowed in.</p> <p>When <code>allowas-in-enable</code> is disabled, your AS number is only allowed to appear once in an <code>AS_PATH</code>.</p> <p>.</p> | unset |
| <code>allowas-in6</code> <max_num_AS_integer> | <p>This field is available when <code>allowas-in-enable6</code> is set to <code>enable</code>.</p> <p>When <code>allowas-in-enable6</code> is disabled, your AS number is only allowed to appear once in an <code>AS_PATH</code>.</p> <p>Set the maximum number of occurrences your AS number is allowed in.</p> | unset |
| <code>allowas-in-enable</code> {enable disable} | Enable or disable the readvertising of all prefixes containing duplicate AS numbers. Set the amount of time that must expire before readvertising through the <code>allowas-in</code> field. | disable |
| <code>allowas-in-enable6</code> {enable disable} | Enable or disable the readvertising of all prefixes containing duplicate AS numbers. Set the amount of time that must expire before readvertising through the <code>allowas-in6</code> field. | disable |
| <code>as-override</code> {enable disable} | Enable or disable BGP AS override (for IPv4 traffic). | disable |
| <code>as-override6</code> {enable disable} | Enable or disable BGP AS override (for IPv6 traffic). | disable |
| <code>attribute-unchanged</code> [as-path] [med] [next-hop] | <p>Propagate unchanged BGP attributes to the BGP neighbor.</p> <ul style="list-style-type: none"> To advertise unchanged <code>AS_PATH</code> attributes, select <code>as-path</code>. To advertise unchanged <code>MULTI_EXIT_DISC</code> attributes, select <code>med</code>. To advertise the IP address of the next-hop router interface (even when the address has not changed), select <code>next-hop</code>. An empty set is a supported value. | Empty set. |

| Variable | Description | Default |
|--|---|------------|
| attribute-unchanged6 [as-path] [med] [next-hop] | Propagate unchanged BGP attributes to the BGP neighbor. <ul style="list-style-type: none"> To advertise unchanged AS_PATH attributes, select <code>as-path</code>. To advertise unchanged MULTI_EXIT_DISC attributes, select <code>med</code>. To advertise the IP address of the next-hop router interface (even when the address has not changed), select <code>next-hop</code>. An empty set is a supported value. | Empty set. |
| bfd {enable disable} | Enable to turn on Bi-Directional Forwarding Detection (BFD) for this neighbor. This indicates that this neighbor is using BFD. | disable |
| capability-default-originate {enable disable} | Enable or disable the advertising of the default route to BGP neighbors. | disable |
| capability-default-originate6 {enable disable} | Enable or disable the advertising of the default route to IPv6 BGP neighbors. | disable |
| capability-dynamic {enable disable} | Enable or disable the advertising of dynamic capability to BGP neighbors. | disable |
| capability-graceful-restart {enable disable} | Enable or disable the advertising of graceful-restart capability to BGP neighbors. | disable |
| capability-graceful-restart6 {enable disable} | Enable or disable the advertising of graceful-restart capability to IPv6 BGP neighbors. | disable |
| capability-orf {both none receive send} | Enable advertising of Outbound Routing Filter (ORF) prefix-list capability to the BGP neighbor. Choose one of: both — enable send and receive capability. receive — enable receive capability. send — enable send capability. none — disable the advertising of ORF prefix-list capability. • | disable |
| capability-orf6 {both none receive send} | Enable advertising of IPv6 ORF prefix-list capability to the BGP neighbor. Choose one of: both — enable send and receive capability. receive — enable receive capability. send — enable send capability. none — disable the advertising of IPv6 ORF prefix-list capability. | disable |
| capability-route-refresh {enable disable} | Enable or disable the advertising of route-refresh capability to the BGP neighbor. | enable |

| Variable | Description | Default |
|---|---|---------------|
| connect-timer <seconds_integer> | Set the maximum amount of time (in seconds) that the FortiGate unit waits to make a connection with a BGP neighbor before the neighbor is declared unreachable. The range is from 0 to 65 535. | - 1 (not set) |
| default-originate-routemap <routemap_str> | Advertise a default route out from the FortiGate unit to this neighbor using a route_map named <routemap_str>. The route_map name can be up to 35 characters long and is defined using the config router route_map command. For more information, see “router route-map” on page 438 . | Null. |
| default-originate-routemap6 <routemap_str> | Advertise a default route out from the FortiGate unit to this neighbor using a route_map named <routemap_str>. The route_map name can be up to 35 characters long and is defined using the config router route_map command. | Null. |
| description <text_str> | Enter a one-word (no spaces) description to associate with the BGP neighbor configuration settings. | Null. |
| distribute-list-in <access-list-name_str> | Limit route updates from the BGP neighbor based on the Network Layer Reachability Information (NLRI) defined in the specified access list. You must create the access list before it can be selected here. See “router access-list, access-list6” on page 342 . | Null. |
| distribute-list-in6 <access-list-name_str> | Limit route updates from the IPv6 BGP neighbor based on the Network Layer Reachability Information (NLRI) defined in the specified access list. You must create the access list before it can be selected here. See “router access-list, access-list6” on page 342 . | Null |
| distribute-list-out <access-list-name_str> | Limit route updates to the BGP neighbor based on the NLRI defined in the specified access list. You must create the access list before it can be selected here. See “router access-list, access-list6” on page 342 . | Null. |
| distribute-list-out6 <access-list-name_str> | Limit route updates to the IPv6 BGP neighbor based on the NLRI defined in the specified access list. You must create the access list before it can be selected here. See “router access-list, access-list6” on page 342 . | Null |
| dont-capability-negotiate { enable disable } | Enable or disable capability negotiations with the BGP neighbor. | disable |
| ebgp-enforce-multihop { enable disable } | Enable or disable the enforcement of Exterior BGP (EBGP) multihops. | disable |
| ebgp-multihop-ttl <seconds_integer> | This field is available when ebgp-enforce-multihop is set to enable. Define a TTL value (in hop counts) for BGP packets sent to the BGP neighbor. The range is from 1 to 255. | 255 |

| Variable | Description | Default |
|--|---|--------------|
| filter-list-in <aspath-list-name_str> | Limit inbound BGP routes according to the specified AS-path list. You must create the AS-path list before it can be selected here. See “router aspath-list” on page 344 . | Null. |
| filter-list-in6 <aspath-list-name_str> | Limit inbound IPv6 BGP routes according to the specified AS-path list. You must create the AS-path list before it can be selected here. See “router aspath-list” on page 344 . | Null |
| filter-list-out <aspath-list-name_str> | Limit outbound BGP routes according to the specified AS-path list. You must create the AS-path list before it can be selected here. See “router aspath-list” on page 344 . | Null. |
| filter-list-out6 <aspath-list-name_str> | Limit outbound IPv6 BGP routes according to the specified AS-path list. You must create the AS-path list before it can be selected here. See “router aspath-list” on page 344 . | Null |
| holdtime-timer <seconds_integer> | The amount of time (in seconds) that must expire before the FortiGate unit declares the BGP neighbor down. This value overrides the global <code>holdtime-timer</code> value (see subcommand “config router bgp” on page 351). A keepalive message must be received every <code>seconds_integer</code> from the BGP neighbor or it is declared down. The value can be 0 or an integer in the 3 to 65 535 range. This field is available when <code>graceful-restart</code> is set to <code>enabled</code> . | -1 (not set) |
| interface <interface-name_str> | Specify a descriptive name for the BGP neighbor interface. | Null. |
| keep-alive-timer <seconds_integer> | The frequency (in seconds) that a keepalive message is sent from the FortiGate unit to the BGP neighbor. This value overrides the global <code>keep-alive-timer</code> value (see subcommand “config router bgp” on page 351). The range is from 0 to 65 535. | -1 (not set) |
| maximum-prefix <prefix_integer> | Set the maximum number of NLRI prefixes to accept from the BGP neighbor. When the maximum is reached, the FortiGate unit disconnects the BGP neighbor. The range is from 1 to 4 294 967 295. Changing this value on the FortiGate unit does not disconnect the BGP neighbor. However, if the neighbor goes down because it reaches the maximum number of prefixes and you increase the maximum-prefix value afterward, the neighbor will be reset. | unset |

| Variable | Description | Default |
|---|--|---------|
| maximum-prefix6 <prefix_integer> | Set the maximum number of NLRI prefixes to accept from the IPv6 BGP neighbor. When the maximum is reached, the FortiGate unit disconnects the BGP neighbor. The range is from 1 to 4 294 967 295. Changing this value on the FortiGate unit does not disconnect the BGP neighbor. However, if the neighbor goes down because it reaches the maximum number of prefixes and you increase the maximum-prefix value afterward, the neighbor will be reset. | unset |
| maximum-prefix-threshold <percentage_integer> | This field is available when maximum-prefix is set. Specify the threshold (as a percentage) that must be exceeded before a warning message about the maximum number of NLRI prefixes is displayed. The range is from 1 to 100. | 75 |
| maximum-prefix-threshold6 <percentage_integer> | This field is available when maximum-prefix6 is set. Specify the threshold (as a percentage) that must be exceeded before a warning message about the maximum number of NLRI prefixes is displayed. The range is from 1 to 100. | 75 |
| maximum-prefix-warning-only {enable disable} | This field is available when maximum-prefix is set. Enable or disable the display of a warning when the maximum-prefix-threshold has been reached. | disable |
| maximum-prefix-warning-only6 {enable disable} | This field is available when maximum-prefix6 is set. Enable or disable the display of a warning when the maximum-prefix-threshold6 has been reached. | disable |
| next-hop-self {enable disable} | Enable or disable advertising of the FortiGate unit's IP address (instead of the neighbor's IP address) in the NEXT_HOP information that is sent to IBGP peers. | disable |
| next-hop-self6 {enable disable} | Enable or disable advertising of the FortiGate unit's IP address (instead of the neighbor's IP address) in the NEXT_HOP information that is sent to IBGP peers. | disable |
| override-capability {enable disable} | Enable or disable IPv6 addressing for a BGP neighbor that does not support capability negotiation. | disable |
| passive {enable disable} | Enable or disable the sending of Open messages to BGP neighbors. | disable |
| password <string> | Enter password used in MD5 authentication to protect BGP sessions. (RFC 2385) | Null. |

| Variable | Description | Default |
|--|--|---------|
| prefix-list-in <prefix-list-name_str> | Limit route updates from a BGP neighbor based on the Network Layer Reachability Information (NLRI) in the specified prefix list. The prefix list defines the NLRI prefix and length advertised in a route. You must create the prefix list before it can be selected here. See “router prefix-list, prefix-list6” on page 421 . | Null. |
| prefix-list-in6 <prefix-list-name_str> | Limit route updates from an IPv6 BGP neighbor based on the Network Layer Reachability Information (NLRI) in the specified prefix list. The prefix list defines the NLRI prefix and length advertised in a route. You must create the prefix list before it can be selected here. See “router prefix-list, prefix-list6” on page 421 . | Null |
| prefix-list-out <prefix-list-name_str> | Limit route updates to a BGP neighbor based on the NLRI in the specified prefix list. The prefix list defines the NLRI prefix and length advertised in a route. You must create the prefix list before it can be selected here. See “router prefix-list, prefix-list6” on page 421 . | Null. |
| prefix-list-out6 <prefix-list-name_str> | Limit route updates to an IPv6 BGP neighbor based on the NLRI in the specified prefix list. The prefix list defines the NLRI prefix and length advertised in a route. You must create the prefix list before it can be selected here. See “router prefix-list, prefix-list6” on page 421 . | Null |
| remote-as <id_integer> | Adds a BGP neighbor to the FortiGate unit configuration and sets the AS number of the neighbor. The range is from 1 to 65 535. If the number is identical to the FortiGate unit AS number, the FortiGate unit communicates with the neighbor using internal BGP (IBGP). Otherwise, the neighbor is an external peer and the FortiGate unit uses EBGP to communicate with the neighbor. | unset |
| remove-private-as {enable disable} | Remove the private AS numbers from outbound updates to the BGP neighbor. | disable |
| remove-private-as6 {enable disable} | Remove the private AS numbers from outbound updates to the IPv6 BGP neighbor. | disable |
| restart_time <seconds_integer> | Sets the time until a restart happens. The time until the restart can be from 0 to 3600 seconds. | 0 |
| retain-stale-time <seconds_integer> | This field is available when <code>capability-graceful-restart</code> is set to <code>enable</code> . Specify the time (in seconds) that stale routes to the BGP neighbor will be retained. The range is from 1 to 65 535. A value of 0 disables this feature. | 0 |
| route-map-in <routemap-name_str> | Limit route updates or change the attributes of route updates from the BGP neighbor according to the specified route map. You must create the route-map before it can be selected here. See “route-map” on page 438 and “Using route maps with BGP” on page 440 . | Null. |

| Variable | Description | Default |
|---|--|---------|
| route-map-in6 <route-map-name_str> | Limit route updates or change the attributes of route updates from the IPv6 BGP neighbor according to the specified route map. You must create the route-map before it can be selected here. | Null |
| route-map-out <route-map-name_str> | Limit route updates or change the attributes of route updates to the BGP neighbor according to the specified route map. You must create the route-map before it can be selected here. See “route-map” on page 438 and “Using route maps with BGP” on page 440 . | Null. |
| route-map-out6 <route-map-name_str> | Limit route updates or change the attributes of route updates to the IPv6 BGP neighbor according to the specified route map. You must create the route-map before it can be selected here. | Null |
| route-reflector-client {enable disable} | This field is available when <code>remote-as</code> is identical to the FortiGate unit AS number (see “as <local_as_id>” on page 351). Enable or disable the operation of the FortiGate unit as a route reflector and identify the BGP neighbor as a route-reflector client. Inbound routes for route reflectors can change the <code>next-hop</code> , <code>local-preference</code> , <code>med</code> , and <code>as-path</code> attributes of IBGP routes for local route selection, while outbound IBGP routes do not take into effect these attributes. | disable |
| route-reflector-client6 {enable disable} | This field is available when <code>remote-as</code> is identical to the FortiGate unit AS number. Enable or disable the operation of the FortiGate unit as a route reflector and identify the BGP neighbor as a route-reflector client. Inbound routes for route reflectors can change the <code>next-hop</code> , <code>local-preference</code> , <code>med</code> , and <code>as-path</code> attributes of IBGP routes for local route selection, while outbound IBGP routes do not take into effect these attributes. | disable |
| route-server-client {enable disable} | Enable or disable the recognition of the BGP neighbor as route-server client. | disable |
| route-server-client6 {enable disable} | Enable or disable the recognition of the IPv6 BGP neighbor as route-server client. | disable |
| send-community {both disable extended standard} | Enable sending the COMMUNITY attribute to the BGP neighbor. Choose one of: standard — advertise standard capabilities. extended — advertise extended capabilities. both — advertise extended and standard capabilities. disable — disable the advertising of the COMMUNITY attribute. | both |

| Variable | Description | Default |
|--|---|---------|
| send-community6 {both disable extended standard} | Enable sending the COMMUNITY attribute to the IPv6 BGP neighbor. Choose one of: standard — advertise standard capabilities extended — advertise extended capabilities both — advertise extended and standard capabilities disable — disable the advertising of the COMMUNITY attribute. | both |
| shutdown {enable disable} | Administratively enable or disable the BGP neighbor. | disable |
| soft-reconfiguration {enable disable} | Enable or disable the FortiGate unit to store unmodified updates from the BGP neighbor to support inbound soft-reconfiguration. | disable |
| soft-reconfiguration6 {enable disable} | Enable or disable the FortiGate unit to store unmodified updates from the IPv6 BGP neighbor to support inbound soft-reconfiguration. | disable |
| strict-capability-match {enable disable} | Enable or disable strict-capability negotiation matching with the BGP neighbor. | disable |
| unsuppress-map <route-map-name_str> | Specify the name of the route-map to selectively unsuppress suppressed routes. You must create the route-map before it can be selected here. See “route-map” on page 438 and “Using route maps with BGP” on page 440 . | Null. |
| unsuppress-map6 <route-map-name_str> | Specify the name of the route-map to selectively unsuppress suppressed IPv6 routes. You must create the route-map before it can be selected here. | Null |
| update-source <interface-name_str> | Specify the name of the local FortiGate unit interface to use for TCP connections to neighbors. The IP address of the interface will be used as the source address for outgoing updates. | Null. |
| weight <weight_integer> | Apply a weight value to all routes learned from a neighbor. A higher number signifies a greater preference. The range is from 0 to 65 535. | unset |

Example

This example shows how to set the AS number of a BGP neighbor at IP address 10.10.10.167 and enter a descriptive name for the configuration.

```

config router bgp
  config neighbor
    edit 10.10.10.167
      set remote-as 2879
      set description BGP_neighbor_Site1
    end
  end
end

```

config network, config network6

Use this subcommand to set or unset BGP network configuration parameters. The subcommand is used to advertise a BGP network (that is, an IP prefix) — you specify the IP addresses making up the local BGP network. Use `config network6` for IPv6 routing.

When you enable the `network-import-check` attribute in the `config router bgp` subcommand, (see [“network-import-check {disable | enable}” on page 354](#)) and you specify a BGP network prefix through the `config network` subcommand, the FortiGate unit searches its routing table for a matching entry. If an exact match is found, the prefix is advertised. A route-map can optionally be used to modify the attributes of routes before they are advertised.

The `prefix` field is required. All other fields are optional.

| Variable | Description | Default |
|--|--|--------------------|
| <code>edit <network_id></code> | Enter an ID number for the entry. The number must be an integer. | No default. |
| <code>backdoor {enable disable}</code> | Enable or disable the route as a backdoor, which causes an administrative distance of 200 to be assigned to the route. Backdoor routes are not advertised to EBGp peers. | disable |
| <code>prefix <address_ipv4mask></code> | Enter the IP address and netmask that identifies the BGP network to advertise. | 0.0.0.0 0.0.0.0 |
| <code>prefix6 <address_ipv6mask></code> | Enter the IP address and netmask that identifies the BGP network to advertise. | ::/0 |
| <code>route-map <routermap- name_str></code> | Specify the name of the route-map that will be used to modify the attributes of the route before it is advertised. You must create the route-map before it can be selected here. See “route-map” on page 438 and “Using route maps with BGP” on page 440 . | Null. |

Example

This example defines a BGP network at IP address 10.0.0.0/8. A route map named `BGP_rmap1` is used to modify the attributes of the local BGP routes before they are advertised.

```
config router bgp
  config network
    edit 1
      set prefix 10.0.0.0/8
      set route-map BGP_rmap1
    end
  end

config router route-map
  edit BGP_rmap1
    config rule
      edit 1
        set set-community no-export
      end
    end
  end
```

config redistribute, config redistribute6

Use this subcommand to set or unset BGP redistribution table parameters. Use `config redistribute6` for IPv6 routing. You can enable BGP to provide connectivity between connected, static, RIP, and/or OSPF routes. BGP redistributes the routes from one protocol to another. When a large internetwork is divided into multiple routing domains, use the subcommand to redistribute routes to the various domains. As an alternative, you can use the `config network` subcommand to advertise a prefix to the BGP network (see [“config network, config network6” on page 365](#)).

The BGP redistribution table contains four static entries. You cannot add entries to the table. The entries are defined as follows:

- `connected` — Redistribute routes learned from a direct connection to the destination network.
- `isis` — Redistribute routes learned from ISIS.
- `static` — Redistribute the static routes defined in the FortiGate unit routing table.
- `rip` — Redistribute routes learned from RIP.
- `ospf` — Redistribute routes learned from OSPF.

When you enter the subcommand, end the command with one of the four static entry names (that is, `config redistribute {connected | isis | static | rip | ospf}`).



The `status` and `route-map` fields are optional.

| Variable | Description | Default |
|---|--|---------|
| <code>status {enable disable}</code> | Enable or disable the redistribution of connected, static, RIP, or OSPF routes. | disable |
| <code>route-map <route-map-name_str></code> | Specify the name of the route map that identifies the routes to redistribute. You must create the route map before it can be selected here. See “router route-map” on page 438 and “Using route maps with BGP” on page 440 . If a route map is not specified, all routes are redistributed to BGP. | Null |

Example

The following example changes the `status` and `route-map` fields of the `connected` entry.

```
config router bgp
  config redistribute connected
    set status enable
    set route-map rmap1
  end
end
```

community-list

Use this command to identify BGP routes according to their COMMUNITY attributes (see RFC 1997). Each entry in the community list defines a rule for matching and selecting routes based on the setting of the COMMUNITY attribute. The default rule in a community list (which the FortiGate unit applies last) denies the matching of all routes.

You add a route to a community by setting its COMMUNITY attribute. A route can belong to more than one community. A route may be added to a community because it has something in common with the other routes in the group (for example, the attribute could identify all routes to satellite offices).

When the COMMUNITY attribute is set, the FortiGate unit can select routes based on their COMMUNITY attribute values.

Syntax

```
config router community-list
  edit <community_name>
    set type {standard | expanded}
    config rule
      edit <community_rule_id>
        set action {deny | permit}
        set match <criteria>
        set regexp <regular_expression>
      end
    end
  end
```



The action field is required. All other fields are optional.

| Variable | Description | Default |
|-----------------------------|--|-------------|
| edit <community_name> | Enter a name for the community list. | No default. |
| type {standard expanded} | Specify the type of community to match. If you select expanded, you must also specify a config rule regexp value. See " regexp <regular_expression> " on page 368. | standard |
| config rule variables | | |
| edit <community_rule_id> | Enter an entry number for the rule. The number must be an integer. | No default. |
| action {deny permit} | Deny or permit operations on a route based on the value of the route's COMMUNITY attribute. | No default. |

| Variable | Description | Default |
|---|---|---------|
| <code>match <criteria></code> | <p>This field is available when <code>set type</code> is set to <code>standard</code>.</p> <p>Specify the criteria for matching a reserved community.</p> <ul style="list-style-type: none"> • Use decimal notation to match one or more COMMUNITY attributes having the syntax <code>AA:NN</code>, where <code>AA</code> represents an AS, and <code>NN</code> is the community identifier. Delimit complex expressions with double-quotation marks (for example, <code>"123 : 234 345:456"</code>). • To match all routes in the Internet community, type <code>internet</code>. • To match all routes in the LOCAL_AS community, type <code>local-AS</code>. Matched routes are not advertised locally. • To select all routes in the NO_ADVERTISE community, type <code>no-advertise</code>. Matched routes are not advertised. • To select all routes in the NO_EXPORT community, type <code>no-export</code>. Matched routes are not advertised to EBGp peers. If a confederation is configured, the routes are advertised within the confederation. | Null |
| <code>regex <regular_expression></code> | <p>This field is available when <code>set type</code> is set to <code>expanded</code>.</p> <p>Specify an ordered list of COMMUNITY attributes as a regular expression. The value or values are used to match a community. Delimit a complex <code>regular_expression</code> value using double-quotation marks.</p> | Null |

gwdetect

Use this command to verify a valid connection with one or more servers.

Dead gateway detection, or interface status detection, consists of the unit confirming that packets sent from an interface result in a response from a server. You can use up to three different protocols to confirm that an interface can connect to the server. Usually the server is the next-hop router that leads to an external network or the Internet. Interface status detection sends a packet using the configured protocols. If a response is received from the server, the unit assumes the interface can connect to the network. If a response is not received, the unit assumes that the interface cannot connect to the network.

Syntax

```
config router gwdetect
  edit <index_ID>
    set failtime <attempts_int>
    set gateway-ip <IPv4_addr>
    set ha-priority <priority_int>
    set interface <interface_name>
    set interval <seconds_int>
    set protocol {ping | tcp-echo | udp-echo}
    set server <servername_string>
    set source-ip <ipv4_addr>
  end
```

The **action** field is required. All other fields are optional.

| Variable | Description | Default |
|---------------------------------------|--|-------------|
| edit <index_ID> | Enter an integer ID for this gwdetect entry. | No default. |
| failtime <attempts_int> | Enter the number of failed attempts to contact the server for declaring the ping server lost. | 5 |
| gateway-ip <IPv4_addr> | Enter the IP address of the gateway used to ping the server. | 0.0.0.0 |
| ha-priority <priority_int> | Select the HA election priority. Valid range is 1 to 50. The default is 1. This setting is not synchronized by HA. | 1 |
| interface <interface_name> | Specify the interface that connects to the server. | null |
| interval <seconds_int> | Enter the seconds between attempts to contact the server. | 5 |
| protocol {ping tcp-echo udp-echo} | Select the protocol to be used when contacting the server. | ping |
| server <servername_string> | Enter the server name. It must comply with RFC1035. | No default. |
| source-ip <ipv4_addr> | Enter the IP address that is checking the gateway. If none is selected, one will be automatically selected from the interface | 0.0.0.0 |

isis

IS-IS is described in [RFC 1142](#). You can enable and configure IS-IS on your FortiGate unit if this routing protocol is in use on your network.



For each routing protocol, you can also use a `redistribute` command to redistribute IS-IS routes with the other protocol. For example, to redistribute IS-IS routes over OSPF enter:

```
config router ospf
  config redistribute isis
    set status enable
  end
end
```

```
config router isis
  set adjacency-check {enable | disable}
  set auth-keychain-l1 <keychain_str>
  set auth-keychain-l2 <keychain_str>
  set auth-mode-l1 {md5 | password}
  set auth-mode-l2 {md5 | password}
  set auth-password-l1 <password>
  set auth-password-l2 <password>
  set auth-sendonly-l1 {enable | disable}
  set auth-sendonly-l2 {enable | disable}
  set default-originate {enable | disable}
  set dynamic-hostname {enable | disable}
  set ignore-lsp-errors {enable | disable}
  set is-type {level-1 | level-1-2 | level-2-only}
  set lsp-gen-interval-l1 <interval_int>
  set lsp-gen-interval-l2 <interval_int>
  set lsp-refresh-interval <interval_int>
  set max-lsp-lifetime <lifetime_int>
  set metric-style {narrow | narrow-transition | narrow-transition-
    l1 | narrow-transition-l2 | transition | transition-l1
    | transition-l2 | wide | wide-l1 | wide-l2 | wide-transition
    | wide-transition-l1 | wide-transition-l2}
  set overload-bit {enable | disable}
  set overload-bit-on-startup
  set overload-bit-suppress external interlevel
  set redistribute-l1 {enable | disable}
  set redistribute-l1-list <access_list_str>
  set redistribute-l2 {enable | disable}
  set redistribute-l2-list <access_list_str>
  set spf-interval-exp-l1 <min_delay_int> <max_delay_int>
  set spf-interval-exp-l2 <min_delay_int> <max_delay_int>
```

```
config isis-interface
  edit <interface_str>
    set auth-keychain-l1 <keychain_str>
    set auth-keychain-l2 <keychain_str>
    set auth-mode-l1 {md5 | password}
    set auth-mode-l2 {md5 | password}
    set auth-password-l1 <password>
    set auth-password-l2 <password>
    set auth-send-only-l1 {enable | disable}
    set auth-send-only-l2 {enable | disable}
    set circuit-type {level-1 | level-1-2 | level-2-only}
    set csnp-interval-l1 <interval_int>
    set csnp-interval-l2 <interval_int>
    set hello-interval-l1 <interval_int>
    set hello-interval-l2 <interval_int>
    set hello-multiplier-l1 <multiplier_int>
    set hello-multiplier-l2 <multiplier_int>
    set hello-padding {enable | disable}
    set lsp-interval <interval_int>
    set lsp-retransmit-interval <interval_int>
    set mesh-group {enable | disable}
    set mesh-group-id <id_int>
    set metric-l1 <metric_int>
    set metric-l2 <metric_int>
    set network-type {broadcast | point-to-point}
    set priority-l1 <priority_int>
    set priority-l2 <priority_int>
    set status {enable | disable}
    set wide-metric-l1 <metric_int>
    set wide-metric-l2 <metric_int>
  config isis-net
    edit <id>
      set net <user_defined>
    config redistribute {bgp | connected | ospf | rip | static}
      set status {enable | disable}
      set metric <metric_int>
      set metric-type {external | internal}
      set level {level-1 | level-1-2 | level-2}
      set routemap <routemap_name>
    config summary-address
      edit <id>
        set level {level-1 | level-1-2 | level-2}
        set prefix <prefix_ipv4> <prefix_mask>
      end
    end
  end
```

| Variable | Description | Default |
|--|--|-----------|
| adjacency-check { enable disable } | Enable to check neighbor protocol support. | disable |
| auth-keychain-l1 <keychain_str> | Authentication key-chain for level 1 PDUs. Available when auth-mode-l1 is set to md5. | |
| auth-keychain-l2 <keychain_str> | Authentication key-chain for level 2 PDUs. Available when auth-mode-l2 is set to md5. | |
| auth-mode-l1 { md5 password } | Level 1 authentication mode. | password |
| auth-mode-l2 { md5 password } | Level 2 authentication mode. | password |
| auth-password-l1 <password> | Authentication password for level 1 PDUs. Available when auth-keychain-11 is set to password. | |
| auth-password-l2 <password> | Authentication password for level 2 PDUs. Available when auth-keychain-12 is set to password. | |
| auth-sendonly-l1 { enable disable } | Level 1 authentication send-only. | disable |
| auth-sendonly-l2 { enable disable } | Level 2 authentication send-only. | disable |
| default-originate { enable disable } | Control distribution of default information. | disable |
| dynamic-hostname { enable disable } | Enable dynamic hostname. | disable |
| ignore-lsp-errors { enable disable } | Enable to ignore LSPs with bad checksums. | disable |
| is-type { level-1 level-1-2 level-2-only } | Set the ISIS level to use. IS-IS routers are designated as being: Level 1 (intra-area); Level 2 (inter area); or Level 1-2 (both). | level-1-2 |
| lsp-gen-interval-l1 <interval_int> | Minimum interval for level 1 link state packet (LSP) regenerating. Range 1 to 120. | 30 |
| lsp-gen-interval-l2 <interval_int> | Minimum interval for level 2 LSP regenerating. Range 1 to 120. | 30 |
| lsp-refresh-interval <interval_int> | LSP refresh time in seconds. Range 1 to 65535 seconds. | 900 |
| max-lsp-lifetime <lifetime_int> | Maximum LSP lifetime in seconds. Range 350 to 65535 seconds. | 1200 |

| Variable | Description | Default |
|---|---|-----------|
| metric-style { narrow narrow-transition narrow-transition-l1 narrow-transition-l2 transition transition- l1 transition-l2 wide wide-l1 wide-l2 wide-transition wide-transition-l1 wide-transition-l2 } | Use old-style (ISO 10589) or new-style packet formats. <ul style="list-style-type: none"> • narrow Use old style of TLVs with narrow metric. • narrow-transition narrow, and accept both styles of TLVs during transition. • narrow-transition-l1 narrow-transition level-1 only. • narrow-transition-l2 narrow-transition level-2 only. • transition Send and accept both styles of TLVs during transition. • transition-l1 transition level-1 only. • transition-l2 transition level-2 only. • wide Use new style of TLVs to carry wider metric. • wide-l1 wide level-1 only. • wide-l2 wide level-2 only. • wide-transition wide, and accept both styles of TLVs during transition. • wide-transition-l1 wide-transition level-1 only. • wide-transition-l2 wide-transition level-2 only. | narrow |
| overload-bit { enable disable } | Signal other routers not to use us in SPF. | disable |
| overload-bit-on-startup | Set overload-bit only temporarily after reboot. Range is 5-86400 seconds. Enter <code>unset overload-bit-on-startup</code> to disable. Entering <code>set overload-bit-on-startup 0</code> is invalid. | 0 |
| overload-bit-suppress external interlevel | Suppress overload-bit for the specific prefixes. You can suppress the overload-bit for external prefixes, internal prefixes or both. Enter <code>unset overload-bit-suppress</code> to disable. | |
| redistribute-l1 { enable disable } | Redistribute level 1 routes into level 2. If enabled, configure <code>redistribute-l1-list</code> . | disable |
| redistribute-l1-list <access_list_str> | Access-list for redistribute l1 to l2. Available if <code>redistribute-l1</code> enabled. | (null) |
| redistribute-l2 { enable disable } | Redistribute level 2 routes into level 1. If enabled, configure <code>redistribute-l2-list</code> . | disable |
| redistribute-l2-list <access_list_str> | Access-list for redistribute l2 to l1. Available if <code>redistribute-l2</code> enabled. | (null) |
| spf-interval-exp-l1 <min_delay_int> <max_delay_int> | Level 1 SPF calculation delay in milliseconds. Enter the maximum and maximum delay between receiving a change to the level 1 SPF calculation in milliseconds. | 500 50000 |
| spf-interval-exp-l2 <min_delay_int> <max_delay_int> | Level 2 SPF calculation delay. Enter the maximum and maximum delay between receiving a change to the level 2 SPF calculation in milliseconds. | 500 50000 |

config isis-interface

Configure and enable FortiGate unit interfaces for IS-IS.

| Variable | Description | Default |
|---|---|-----------|
| edit <interface_str> | Edit an IS-IS interface. | |
| auth-keychain-l1 <keychain_str> | Authentication key-chain for level 1 PDUs. Available when auth-mode-l1 is set to md5. | |
| auth-keychain-l2 <keychain_str> | Authentication key-chain for level 2 PDUs. Available when auth-mode-l2 is set to md5. | |
| auth-mode-l1 {md5 password} | Level 1 authentication mode. | password |
| auth-mode-l2 {md5 password} | Level 2 authentication mode. | password |
| auth-password-l1 <password> | Authentication password for level 1 PDUs. Available when auth-keychain-11 is set to password. | |
| auth-password-l2 <password> | Authentication password for level 2 PDUs. Available when auth-keychain-12 is set to password. | |
| auth-send-only-l1 {enable disable} | Level 1 authentication send-only. | disable |
| auth-send-only-l2 {enable disable} | Level 2 authentication send-only. | disable |
| circuit-type {level-1 level-1-2 level-2-only} | Set the ISIS circuit type to use for the interface. IS-IS routers are designated as being: Level 1 (intra-area); Level 2 (inter area); or Level 1-2 (both). | level-1-2 |
| csnp-interval-l1 <interval_int> | Level 1 CSNP interval. The range is 1-65535 seconds. | 10 |
| csnp-interval-l2 <interval_int> | Level 2 CSNP interval. The range is 1-65535 seconds. | 10 |
| hello-interval-l1 <interval_int> | Level 1 hello interval. The range is 1-65535 seconds. Set to 0 for a one-second hold time. | 10 |
| hello-interval-l2 <interval_int> | Level 2 hello interval. The range is 1-65535 seconds. Set to 0 for a one-second hold time. | 10 |
| hello-multiplier-l1 <multiplier_int> | Level 1 multiplier for Hello holding time. The range is 2 to 100. | 3 |
| hello-multiplier-l2 <multiplier_int> | Level 2 multiplier for Hello holding time. The range is 2 to 100. | 3 |
| hello-padding {enable disable} | Enable or disable adding padding to IS-IS hello packets. | disable |
| lsp-interval <interval_int> | LSP transmission interval (milliseconds). The range is 1-4294967295. | 33 |
| lsp-retransmit-interval <interval_int> | LSP retransmission interval (seconds). The range is 1-65535. | 5 |
| mesh-group {enable disable} | Enable IS-IS mesh group. | disable |
| mesh-group-id <id_int> | Mesh group ID. The range is 0-4294967295. A value of 0 means the mesh group is blocked. | 0 |
| metric-l1 <metric_int> | Level 1 metric for interface. The range is 1-63. | 10 |
| metric-l2 <metric_int> | Level 2 metric for interface. The range is 1-63. | 10 |

| Variable | Description | Default |
|---|---|---------|
| network-type {broadcast point-to-point} | Set the IS-IS interface's network type. | |
| priority-11 <priority_int> | Level 1 priority. The range is 0-127. | 64 |
| priority-12 <priority_int> | Level 2 priority. The range is 0-127. | 64 |
| status {enable disable} | Enable the interface for IS-IS. | disable |
| wide-metric-11 <metric_int> | Level 1 wide metric for the interface. The range is 1-16777214. | 10 |
| wide-metric-12 <metric_int> | Level 2 wide metric for the interface. The range is 1-16777214. | 10 |

config isis-net

Add IS-IS networks.

| Variable | Description | Default |
|--------------------|--|---------|
| edit <id> | Add the ID number of the IS-IS network | |
| net <user_defined> | Enter a user defined IS-IS network in the form xx.xxxx.xxxx.xx. | : |

config redistribute {bgp | connected | ospf | rip | static}

Redistribute routes from other routing protocols using IS-IS.

| Variable | Description | Default |
|--|---|----------|
| status {enable disable} | Enable or disable redistributing the selected protocol's routes. | disable |
| protocol {bgp connected ospf rip static} | The name of the protocol that to redistribute ISIS routes to. | |
| metric <metric_int> | Set the metric. Range is 0-4261412864. | 0 |
| metric-type {external internal} | Set the metric type. | internal |
| level {level-1 level-1-2 level-2} | Set the ISIS level type to use for distributing routes. IS-IS routers are designated as being: Level 1 (intra-area); Level 2 (inter area); or Level 1-2 (both). | level-2 |
| routemap <routemap_name> | Enter a routemap name. | (null) |

config summary-address

Add IS-IS summary addresses.

| Variable | Description | Default |
|---|---|--------------------|
| edit <id> | Add the ID number of the summary address. | |
| level {level-1 level-1-2 level-2} | Set the ISIS level to use for the summary database. IS-IS routers are designated as being: Level 1 (intra-area); Level 2 (inter area); or Level 1-2 (both). | level-2 |
| prefix <prefix_ipv4> <prefix_mask> | The summary address prefix and netmask. | 0.0.0.0 0.0.0.0 |

key-chain

Use this command to manage RIP version 2 authentication keys. You can add, edit or delete keys identified by the specified key number.

RIP version 2 uses authentication keys to ensure that the routing information exchanged between routers is reliable. For authentication to work, both the sending and receiving routers must be set to use authentication, and must be configured with the same keys.

A key chain is a list of one or more keys and the send and receive lifetimes for each key. Keys are used for authenticating routing packets only during the specified lifetimes. The FortiGate unit migrates from one key to the next according to the scheduled send and receive lifetimes. The sending and receiving routers should have their system dates and times synchronized, but overlapping the key lifetimes ensures that a key is always available even if there is some difference in the system times. For how to to ensure that the FortiGate unit system date and time are correct, see [“config system global” on page 243](#) .

Syntax

```
config router key-chain
  edit <key_chain_name>
    config key
      edit <key_id>
        set accept-lifetime <start> <end>
        set key-string <password>
        set send-lifetime <start> <end>
      end
    end
  end
```



The accept-lifetime, key-string, and send-lifetime fields are required.

| Variable | Description | Default |
|-----------------------|--|-------------|
| edit <key_chain_name> | Enter a name for the key chain list. | No default. |
| config key variables | | |
| edit <key_id> | Enter an ID number for the key entry. The number must be an integer. | No default. |

| Variable | Description | Default |
|-------------------------------|--|-------------|
| accept-lifetime <start> <end> | <p>Set the time period during which the key can be received. The <code>start</code> time has the syntax <code>hh:mm:ss day month year</code>. The <code>end</code> time provides a choice of three settings:</p> <p>hh:mm:ss day month year</p> <p><integer> — a duration from 1 to 2147483646 seconds</p> <p>infinite — for a key that never expires</p> <p>The valid settings for hh:mm:ss day month year are:</p> <p>hh — 0 to 23</p> <p>mm — 0 to 59</p> <p>ss — 0 to 59</p> <p>day — 1 to 31</p> <p>month — 1 to 12</p> <p>year — 1993 to 2035</p> <p>Note: A single digit will be accepted for hh, mm, ss, day, or month fields.</p> | No default. |
| key-string <password> | The <password_str> can be up to 35 characters long. | No default. |
| send-lifetime <start> <end> | <p>Set the time period during which the key can be sent. The <code>start</code> time has the syntax <code>hh:mm:ss day month year</code>. The <code>end</code> time provides a choice of three settings:</p> <p>hh:mm:ss day month year</p> <p><integer> — a duration from 1 to 2147483646 seconds</p> <p>infinite — for a key that never expires</p> <p>The valid settings for hh:mm:ss day month year are:</p> <p>hh — 0 to 23</p> <p>mm — 0 to 59</p> <p>ss — 0 to 59</p> <p>day — 1 to 31</p> <p>month — 1 to 12</p> <p>year — 1993 to 2035</p> <p>Note: A single digit will be accepted for hh, mm, ss, day, or month fields.</p> | No default. |

multicast

A FortiGate unit can operate as a Protocol Independent Multicast (PIM) version 2 router. FortiGate units support PIM sparse mode (RFC 4601) and PIM dense mode (RFC 3973) and can service multicast servers or receivers on the network segment to which a FortiGate unit interface is connected. Multicast routing is not supported in Transparent mode (TP mode).



To support PIM communications, the sending/receiving applications and all connecting PIM routers in between must be enabled with PIM version 2. PIM can use static routes, RIP, OSPF, or BGP to forward multicast packets to their destinations. To enable source-to-destination packet delivery, either sparse mode or dense mode must be enabled on the PIM-router interfaces. Sparse mode routers cannot send multicast messages to dense mode routers. In addition, if a FortiGate unit is located between a source and a PIM router, two PIM routers, or is connected directly to a receiver, you must create a firewall policy manually to pass encapsulated (multicast) packets or decapsulated data (IP traffic) between the source and destination.

A PIM domain is a logical area comprising a number of contiguous networks. The domain contains at least one Boot Strap Router (BSR), and if sparse mode is enabled, a number of Rendezvous Points (RPs) and Designated Routers (DRs). When PIM is enabled on a FortiGate unit, the FortiGate unit can perform any of these functions at any time as configured.

Sparse mode

Initially, all candidate BSRs in a PIM domain exchange bootstrap messages to select one BSR to which each RP sends the multicast address or addresses of the multicast group(s) that it can service. The selected BSR chooses one RP per multicast group and makes this information available to all of the PIM routers in the domain through bootstrap messages. PIM routers use the information to build packet distribution trees, which map each multicast group to a specific RP. Packet distribution trees may also contain information about the sources and receivers associated with particular multicast groups.



When a FortiGate unit interface is configured as a multicast interface, sparse mode is enabled on it by default to ensure that distribution trees are not built unless at least one downstream receiver requests multicast traffic from a specific source. If the sources of multicast traffic and their receivers are close to each other and the PIM domain contains a dense population of active receivers, you may choose to enable dense mode throughout the PIM domain instead.

An RP represents the root of a non-source-specific distribution tree to a multicast group. By joining and pruning the information contained in distribution trees, a single stream of multicast packets (for example, a video feed) originating from the source can be forwarded to a certain RP to reach a multicast destination.

Each PIM router maintains a Multicast Routing Information Base (MRIB) that determines to which neighboring PIM router join and prune messages are sent. An MRIB contains reverse-path information that reveals the path of a multicast packet from its source to the PIM router that maintains the MRIB.

To send multicast traffic, a server application sends IP traffic to a multicast group address. The locally elected DR registers the sender with the RP that is associated with the target multicast group. The RP uses its MRIB to forward a single stream of IP packets from the source to the members of the multicast group. The IP packets are replicated only when necessary to distribute the data to branches of the RP's distribution tree.

To receive multicast traffic, a client application can use Internet Group Management Protocol (IGMP) version 1 (RFC 1112), 2 (RFC 2236), or 3 (RFC 3376) control messages to request the traffic for a particular multicast group. The locally elected DR receives the request and adds the

host to the multicast group that is associated with the connected network segment by sending a join message towards the RP for the group. Afterward, the DR queries the hosts on the connected network segment continually to determine whether the hosts are active. When the DR no longer receives confirmation that at least one member of the multicast group is still active, the DR sends a prune message towards the RP for the group.

Dense mode

The packet organization used in sparse mode is also used in dense mode. When a multicast source begins to send IP traffic and dense mode is enabled, the closest PIM router registers the IP traffic from the multicast source (S) and forwards multicast packets to the multicast group address (G). All PIM routers initially broadcast the multicast packets throughout the PIM domain to ensure that all receivers that have requested traffic for multicast group address G can access the information if needed.

To forward multicast packets to specific destinations afterward, the PIM routers build distribution trees based on the information in multicast packets. Upstream PIM routers depend on prune/graft messages from downstream PIM routers to determine if receivers are actually present on directly connected network segments. The PIM routers exchange state refresh messages to update their distribution trees. FortiGate units store this state information in a Tree Information Base (TIB), which is used to build a multicast forwarding table. The information in the multicast forwarding table determines whether packets are forwarded downstream. The forwarding table is updated whenever the TIB is modified.

PIM routers receive data streams every few minutes and update their forwarding tables using the source (S) and multicast group (G) information in the data stream. Superfluous multicast traffic is stopped by PIM routers that do not have downstream receivers—PIM routers that do not manage multicast groups send prune messages to the upstream PIM routers. When a receiver requests traffic for multicast address G, the closest PIM router sends a graft message upstream to begin receiving multicast packets.

For more information on Multicast routing, see the [FortiGate Multicast Technical Note](#).

Syntax

```
config router multicast
    set igmp-state-limit <limit_integer>
    set multicast-routing {enable | disable}
    set route-limit <limit_integer>
    set route-threshold <threshold_integer>
config interface
    edit <interface_name>
        set cisco-exclude-genid {enable | disable}
        set dr-priority <priority_integer>
        set hello-holdtime <holdtime_integer>
        set hello-interval <hello_integer>
        set multicast-flow <flowname>
        set neighbour-filter <access_list_name>
        set passive {enable | disable}
        set pim-mode {sparse-mode | dense-mode}
        set propagation-delay <delay_integer>
        set rp-candidate {enable | disable}
        set rp-candidate-group <access_list_name>
        set rp-candidate-interval <interval_integer>
        set rp-candidate-priority <priority_integer>
```

```
        set state-refresh-interval <refresh_integer>
        set static-group <flowname>
        set ttl-threshold <ttl_integer>
    end
    config join-group
        edit address <address_ipv4>
    end
    config igmp
        set access-group <access_list_name>
        set immediate-leave-group <access_list_name>
        set last-member-query-count <count_integer>
        set last-member-query-interval <interval_integer>
        set query-interval <interval_integer>
        set query-max-response-time <time_integer>
        set query-timeout <timeout_integer>
        set router-alert-check { enable | disable }
        set version {1 | 2 | 3}
    end
end
config pim-sm-global
    set accept-register-list <access_list_name>
    set bsr-allow-quick-refresh {enable | disable}
    set bsr-candidate {enable | disable}
    set bsr-priority <priority_integer>
    set bsr-interface <interface_name>
    set bsr-hash <hash_integer>
    set cisco-register-checksum {enable | disable}
    set cisco-register-checksum-group <access_list_name>
    set cisco-crp-prefix {enable | disable}
    set cisco-ignore-rp-set-priority {enable | disable}
    set message-interval <interval_integer>
    set register-rate-limit <rate_integer>
    set register-rp-reachability {enable | disable}
    set register-source {disable | interface | ip-address}
    set register-source-interface <interface_name>
    set register-source-ip <address_ipv4>
    set register-suppression <suppress_integer>
    set rp-register-keepalive <keepalive_integer>
    set spt-threshold {enable | disable}
    set spt-threshold-group <access_list_name>
    set ssm {enable | disable}
    set ssm-range <access_list_name>
    config rp-address
        edit <rp_id>
            set ip-address <address_ipv4>
            set group <access_list_name>
        end
    end
end
```

config router multicast

You can configure a FortiGate unit to support PIM using the `config router multicast` CLI command. When PIM is enabled, the FortiGate unit allocates memory to manage mapping information. The FortiGate unit communicates with neighboring PIM routers to acquire mapping information and if required, processes the multicast traffic associated with specific multicast groups.



The end-user multicast client-server applications must be installed and configured to initiate Internet connections and handle broadband content such as audio/video information.

Client applications send multicast data by registering IP traffic with a PIM-enabled router. An end-user could type in a class D multicast group address, an alias for the multicast group address, or a call-conference number to initiate the session.

Rather than sending multiple copies of generated IP traffic to more than one specific IP destination address, PIM-enabled routers encapsulate the data and use the one multicast group address to forward multicast packets to multiple destinations. Because one destination address is used, a single stream of data can be sent. Client applications receive multicast data by requesting that the traffic destined for a certain multicast group address be delivered to them—end-users may use phone books, a menu of ongoing or future sessions, or some other method through a user interface to select the address of interest.

A class D address in the 224.0.0.0 to 239.255.255.255 range may be used as a multicast group address, subject to the rules assigned by the Internet Assigned Numbers Authority (IANA). All class D addresses must be assigned in advance. Because there is no way to determine in advance if a certain multicast group address is in use, collisions may occur (to resolve this problem, end-users may switch to a different multicast address).

To configure a PIM domain

1. If you will be using sparse mode, determine appropriate paths for multicast packets.
2. Make a note of the interfaces that will be PIM-enabled. These interfaces may run a unicast routing protocol.
3. If you will be using sparse mode and want multicast packets to be handled by specific (static) RPs, record the IP addresses of the PIM-enabled interfaces on those RPs.
4. Enable PIM version 2 on all participating routers between the source and receivers. On FortiGate units, use the `config router multicast` command to set global operating parameters.
5. Configure the PIM routers that have good connections throughout the PIM domain to be candidate BSRs.
6. If sparse mode is enabled, configure one or more of the PIM routers to be candidate RPs.
7. If required, adjust the default settings of PIM-enabled interface(s).

All fields are optional.

| Variable | Description | Default |
|---|---|------------|
| igmp-state-limit <limit_integer> | If memory consumption is an issue, specify a limit on the number of IGMP states (multicast memberships) that the FortiGate unit will store. This value represents the maximum combined number of IGMP states (multicast memberships) that can be handled by all interfaces. Traffic associated with excess IGMP membership reports is not delivered. The range is from 96 to 64 000. | 3200 |
| multicast-routing {enable disable} | Enable or disable PIM routing. | disable |
| route-limit <limit_integer> | If memory consumption is an issue, set a limit on the number of multicast routes that can be added to the FortiGate unit routing table. The range is from 1 to 2 147 483 674. | 2147483674 |
| route-threshold <threshold_integer> | Specify the number of multicast routes that can be added to the FortiGate unit's routing table before a warning message is displayed. The route-threshold value must be lower than the route-limit value. The range is from 1 to 2 147 483 674. | 2147483674 |

config interface

Use this subcommand to change interface-related PIM settings, including the mode of operation (sparse or dense). Global settings do not override interface-specific settings.

All fields are optional.

| Variable | Description | Default |
|---|---|-------------|
| edit <interface_name> | Enter the name of the FortiGate unit interface on which to enable PIM protocols. | No default. |
| cisco-exclude-genid {enable disable} | This field applies only when pim-mode is sparse-mode. Enable or disable including a generation ID in hello messages sent to neighboring PIM routers. A GenID value may be included for compatibility with older Cisco IOS routers. | disable |
| dr-priority <priority_integer> | This field applies only when pim-mode is sparse-mode. Assign a priority to FortiGate unit Designated Router (DR) candidacy. The range is from 1 to 4 294 967 294. The value is compared to that of other DR interfaces connected to the same network segment, and the router having the highest DR priority is selected to be the DR. If two DR priority values are the same, the interface having the highest IP address is selected. | 1 |

| Variable | Description | Default |
|---|---|-------------|
| hello-holdtime <holdtime_integer> | Specify the amount of time (in seconds) that a PIM neighbor may consider the information in a hello message to be valid. The range is from 1 to 65 535. If the <code>hello-interval</code> attribute is modified and the <code>hello-holdtime</code> attribute has never been set explicitly, the <code>hello-holdtime</code> attribute is automatically set to 3.5 x <code>hello-interval</code> . | 105 |
| hello-interval <hello_integer> | Set the amount of time (in seconds) that the FortiGate unit waits between sending hello messages to neighboring PIM routers. The range is from 1 to 65 535. Changing the <code>hello-interval</code> attribute may automatically update the <code>hello-holdtime</code> attribute . | 30 |
| multicast-flow <flowname> | Connect the named multicast flow to this interface. Multicast flows are defined in the router multicast-flow command. | No default. |
| neighbour-filter <access_list_name> | Establish or terminate adjacency with PIM neighbors having the IP addresses given in the specified access list. For more information on access lists, see “router access-list, access-list6” on page 342 . | Null |
| passive {enable disable} | Enable or disable PIM communications on the interface without affecting IGMP communications. | disable |
| pim-mode {sparse-mode dense-mode} | Select the PIM mode of operation. Choose one of: sparse-mode — manage PIM packets through distribution trees and multicast groups. dense-mode — enable multicast flooding. | sparse-mode |
| propagation-delay <delay_integer> | This field is available when <code>pim-mode</code> is set to <code>dense-mode</code> . Specify the amount of time (in milliseconds) that the FortiGate unit waits to send prune-override messages. The range is from 100 to 5 000. | 500 |
| rp-candidate {enable disable} | This field is available when <code>pim-mode</code> is set to <code>sparse-mode</code> . Enable or disable the FortiGate unit interface to offer Rendezvous Point (RP) services. | disable |
| rp-candidate-group <access_list_name> | RP candidacy is advertised to certain multicast groups. These groups are based on the multicast group prefixes given in the specified access list. For more information on access lists, see “access-list, access-list6” on page 342 . This field is available when <code>rp-candidate</code> is set to <code>enable</code> and <code>pim-mode</code> is set to <code>sparse-mode</code> . | Null |
| rp-candidate-interval <interval_integer> | This field is available when <code>rp-candidate</code> is set to <code>enable</code> and <code>pim-mode</code> is set to <code>sparse-mode</code> . Set the amount of time (in seconds) that the FortiGate unit waits between sending RP announcement messages. The range is from 1 to 16 383. | 60 |

| Variable | Description | Default |
|---|---|-------------|
| rp-candidate-priority <priority_integer> | <p>This field is available when <code>rp-candidate</code> is set to <code>enable</code> and <code>pim-mode</code> is set to <code>sparse-mode</code>.</p> <p>Assign a priority to FortiGate unit Rendezvous Point (RP) candidacy. The range is from 0 to 255. The BSR compares the value to that of other RP candidates that can service the same multicast group, and the router having the highest RP priority is selected to be the RP for that multicast group. If two RP priority values are the same, the RP candidate having the highest IP address on its RP interface is selected.</p> | 192 |
| state-refresh-interval <refresh_integer> | <p>This field is available when <code>pim-mode</code> is set to <code>dense-mode</code>.</p> <p>This attribute is used when the FortiGate unit is connected directly to the multicast source. Set the amount of time (in seconds) that the FortiGate unit waits between sending state-refresh messages. The range is from 1 to 100. When a state-refresh message is received by a downstream router, the prune state on the downstream router is refreshed.</p> | 60 |
| static-group <flowname> | Statically join this interface to the named multicast group. The interface does not need to have seen any IGMP joins from any host. Multicast flows are defined in the router multicast-flow command. | No default. |
| ttl-threshold <ttl_integer> | <p>Specify the minimum Time-To-Live (TTL) value (in hops) that an outbound multicast packet must have in order to be forwarded from this interface. The range is from 0 to 255.</p> <p>Specifying a high value (for example, 195) prevents PIM packets from being forwarded through the interface.</p> | 1 |
| config join-group variables | | |
| edit address <address_ipv4> | Cause the FortiGate unit interface to activate (IGMP join) the multicast group associated with the specified multicast group address. | No default. |
| config igmp variables | | |
| access-group <access_list_name> | Specify which multicast groups that hosts on the connected network segment may join based on the multicast addresses given in the specified access list. For more information on access lists, see “router access-list, access-list6” on page 342 . | Null. |
| immediate-leave-group <access_list_name> | <p>This field applies when <code>version</code> is set to 2 or 3.</p> <p>Configure a FortiGate unit DR to stop sending traffic and IGMP queries to receivers after receiving an IGMP version 2 group-leave message from any member of the multicast groups identified in the specified access list. For more information on access lists, see “router access-list, access-list6” on page 342.</p> | Null. |

| Variable | Description | Default |
|--|---|----------|
| last-member-query-count <count_integer> | This field applies when <code>version</code> is set to 2 or 3. Specify the number of times that a FortiGate unit DR sends an IGMP query to the last member of a multicast group after receiving an IGMP version 2 group-leave message. | 2 |
| last-member-query-interval <interval_integer> | This field applies when <code>version</code> is set to 2 or 3. Set the amount of time (in milliseconds) that a FortiGate unit DR waits for the last member of a multicast group to respond to an IGMP query. The range is from 1000 to 25 500. If no response is received before the specified time expires and the FortiGate unit DR has already sent an IGMP query <code>last-member-query-count</code> times, the FortiGate unit DR removes the member from the group and sends a prune message to the associated RP. | 1000 |
| query-interval <interval_integer> | Set the amount of time (in seconds) that a FortiGate unit DR waits between sending IGMP queries to determine which members of a multicast group are active. The range is from 1 to 65 535. | 125 |
| query-max-response-time <time_integer> | Set the maximum amount of time (in seconds) that a FortiGate unit DR waits for a member of a multicast group to respond to an IGMP query. The range is from 1 to 25. If no response is received before the specified time expires, the FortiGate unit DR removes the member from the group. | 10 |
| query-timeout <timeout_integer> | Set the amount of time (in seconds) that must expire before a FortiGate unit begins sending IGMP queries to the multicast group that is managed through the interface. The range is from 60 to 300. A FortiGate unit begins sending IGMP queries if it does not receive regular IGMP queries from another DR through the interface. | 255 |
| router-alert-check { enable disable } | Enable to require the Router Alert option in IGMP packets. | disabled |
| version { 1 2 3 } | Specify the version number of IGMP to run on the interface. The value can be 1, 2, or 3. The value must match the version used by all other PIM routers on the connected network segment. | 3 |

config pim-sm-global

These global settings apply only to sparse mode PIM-enabled interfaces. Global PIM settings do not override interface-specific PIM settings.

If sparse mode is enabled, you can configure a DR to send multicast packets to a particular RP by specifying the IP address of the RP through the `config rp-address` variable. The IP address must be directly accessible to the DR. If multicast packets from more than one multicast group can pass through the same RP, you can use an access list to specify the associated multicast group addresses.



To send multicast packets to a particular RP using the `config rp-address` subcommand, the `ip-address` field is required. All other fields are optional.

| Variable | Description | Default |
|--|---|---------|
| <code>accept-register-list</code> <code><access_list_name></code> | Cause a FortiGate unit RP to accept or deny register packets from the source IP addresses given in the specified access list. For more information on access lists, see “router access-list, access-list6” on page 342 . | Null |
| <code>bsr-allow-quick-refresh</code> {enable disable} | Enable or disable accepting BSR quick refresh packets from neighbors. | disable |
| <code>bsr-candidate</code> {enable disable} | Enable or disable the FortiGate unit to offer its services as a Boot Strap Router (BSR) when required. | disable |
| <code>bsr-priority</code> <code><priority_integer></code> | This field is available when <code>bsr-candidate</code> is set to enable. Assign a priority to FortiGate unit BSR candidacy. The range is from 0 to 255. This value is compared to that of other BSR candidates and the candidate having the highest priority is selected to be the BSR. If two BSR priority values are the same, the BSR candidate having the highest IP address on its BSR interface is selected. | 0 |
| <code>bsr-interface</code> <code><interface_name></code> | This field is available when <code>bsr-candidate</code> is set to enable. Specify the name of the PIM-enabled interface through which the FortiGate unit may announce BSR candidacy. | Null |
| <code>bsr-hash</code> <code><hash_integer></code> | This field is available when <code>bsr-candidate</code> is set to enable. Set the length of the mask (in bits) to apply to multicast group addresses in order to derive a single RP for one or more multicast groups. The range is from 0 to 32. For example, a value of 24 means that the first 24 bits of the group address are significant. All multicast groups having the same seed hash belong to the same RP. | 10 |
| <code>cisco-crp-prefix</code> {enable disable} | Enable or disable a FortiGate unit RP that has a group prefix number of 0 to communicate with a Cisco BSR. You may choose to enable the attribute if required for compatibility with older Cisco BSRs. | disable |
| <code>cisco-ignore-rp-set-priority</code> {enable disable} | Enable or disable a FortiGate unit BSR to recognize Cisco RP-SET priority values when deriving a single RP for one or more multicast groups. You may choose to enable the attribute if required for compatibility with older Cisco RPs. | disable |

| Variable | Description | Default |
|---|---|------------|
| cisco-register-checksum { enable disable } | Enable or disable performing a register checksum on entire PIM packets. A register checksum is performed on the header only by default. You may choose to enable register checksums on the whole packet for compatibility with older Cisco IOS routers. | disable |
| cisco-register-checksum-group <access_list_name> | This field is available when <code>cisco-register-checksum</code> is set to <code>enable</code> . Identify on which PIM packets to perform a whole-packet register checksum based on the multicast group addresses in the specified access list. For more information on access lists, see “router access-list, access-list6” on page 342 . You may choose to register checksums on entire PIM packets for compatibility with older Cisco IOS routers. | Null |
| message-interval <interval_integer> | Set the amount of time (in seconds) that the FortiGate unit waits between sending periodic PIM join/prune messages (sparse mode) or prune messages (dense mode). The value must be identical to the message interval value set on all other PIM routers in the PIM domain. The range is from 1 to 65 535. | 60 |
| register-rate-limit <rate_integer> | Set the maximum number of register messages per (S,G) per second that a FortiGate unit DR can send for each PIM entry in the routing table. The range is from 0 to 65 535, where 0 means an unlimited number of register messages per second. | 0 |
| register-rp-reachability {enable disable } | Enable or disable a FortiGate unit DR to check if an RP is accessible prior to sending register messages. | enable |
| register-source {disable interface ip-address } | If the FortiGate unit acts as a DR, enable or disable changing the IP source address of outbound register packets to one of the following IP addresses. The IP address must be accessible to the RP so that the RP can respond to the IP address with a Register-Stop message. Choose one of: disable — retain the IP address of the FortiGate unit DR interface that faces the RP. interface — change the IP source address of a register packet to the IP address of a particular FortiGate unit interface. The <code>register-source-interface</code> attribute specifies the interface name. ip-address — change the IP source address of a register packet to a particular IP address. The <code>register-source-ip</code> attribute specifies the IP address. | ip-address |
| register-source-interface <interface_name> | Enter the name of the FortiGate unit interface. This field is only available when <code>register-source</code> is set to <code>interface</code> . | Null |

| Variable | Description | Default |
|--|---|---------|
| register-source-ip <address_ipv4> | This field is available when <code>register-source</code> is set to <code>address</code> . Enter the IP source address to include in the register message. | 0.0.0.0 |
| register-suppression <suppress_integer> | Enter the amount of time (in seconds) that a FortiGate unit DR waits to start sending data to an RP after receiving a Register-Stop message from the RP. The range is from 1 to 65 535. | 60 |
| rp-register-keepalive <keepalive_integer> | If the FortiGate unit acts as an RP, set the frequency (in seconds) with which the FortiGate unit sends keepalive messages to a DR. The range is from 1 to 65 535. The two routers exchange keepalive messages to maintain a link for as long as the source continues to generate traffic. If the <code>register-suppression</code> attribute is modified on the RP and the <code>rp-register-keepalive</code> attribute has never been set explicitly, the <code>rp-register-keepalive</code> attribute is set to $(3 \times \text{register-suppression}) + 5$ automatically. | 185 |
| spt-threshold {enable disable} | Enable or disable the FortiGate unit to build a Shortest Path Tree (SPT) for forwarding multicast packets. | enable |
| spt-threshold-group <access_list_name> | Build an SPT only for the multicast group addresses given in the specified access list. For more information on access lists, see “router access-list, access-list6” on page 342 . This field is only available when <code>spt-threshold</code> is set to <code>enable</code> . | Null. |
| ssm {enable disable} | This field is available when the IGMP version is set to 3. Enable or disable Source Specific Multicast (SSM) interactions (see RFC 3569). | enable |
| ssm-range <access_list_name> | Enable SSM only for the multicast addresses given in the specified access list. For more information on access lists, see “router access-list, access-list6” on page 342 . By default, multicast addresses in the 232.0.0.0 to 232.255.255.255 (232/8) range are used to support SSM interactions. This field is only available when <code>ssm</code> is set to <code>enable</code> . | Null. |

| Variable | Description | Default |
|------------------------------------|---|-------------|
| config rp-address variables | Only used when <code>pim-mode</code> is <code>sparse-mode</code> . | |
| edit <rp_id> | Enter an ID number for the static RP address entry. The number must be an integer. | No default. |
| ip-address <address_ipv4> | Specify a static IP address for the RP. | 0.0.0.0 |
| group <access_list_name> | <p>Configure a single static RP for the multicast group addresses given in the specified access list. For more information on access lists, see “router access-list, access-list6” on page 342.</p> <p>If an RP for any of these group addresses is already known to the BSR, the static RP address is ignored and the RP known to the BSR is used instead.</p> | Null. |

multicast6

Use this command to configure the FortiGate unit as an IPv6 Protocol Independent Multicast (PIM) version 2 router.

Syntax

```
config router multicast6
    set multicast-routing {enable | disable}
    config interface
        edit <interface_name>
            set hello-holdtime <holdtime_integer>
            set hello-interval <hello_integer>
        end
    config pim-sm-global
        config rp-address
            edit <id_int>
                set ip6-address <ip6_addr>
            end
        end
    end
end
```

| Variable | Description | Default |
|--|---|-------------|
| multicast-routing {enable disable} | Enable or disable IPv6 multicast routing. | disable |
| config interface fields | | |
| edit <interface_name> | Enter the name of the FortiGate unit interface on which to enable PIM protocols. | No default. |
| hello-holdtime <holdtime_integer> | Specify the amount of time (in seconds) that a PIM neighbor may consider the information in a hello message to be valid. The range is from 1 to 65 535. If the hello-interval attribute is modified and the hello-holdtime attribute has never been set explicitly, the hello-holdtime attribute is automatically set to 3.5 x hello-interval. | 105 |
| hello-interval <hello_integer> | Set the amount of time (in seconds) that the FortiGate unit waits between sending hello messages to neighboring PIM routers. The range is from 1 to 65 535. Changing the hello-interval attribute may automatically update the hello-holdtime attribute . | 30 |
| config pim-sm-global / config rp-address fields | | |
| ip6-address <ip6_addr> | Enter the RP router IP address. | :: |

multicast-flow

Use this command to configure the source allowed for a multicast flow when using PIM-SM or PIM-SSM.

Syntax

```
config router multicast-flows
  edit <flowname_str>
    set comments <comment_str>
  config flows
    edit <id>
      set group-addr <group_ipv4>
      set source-addr <src_ipv4>
    end
  end
end
```

| Variable | Description | Default |
|-------------------------|--|---------|
| edit <flowname_str> | Enter a name for this flow. | |
| comments <comment_str> | Optionally, enter a descriptive comment. | |
| edit <id> | Enter the ID number for this flow. | |
| group-addr <group_ipv4> | Enter the multicast group IP address. Range 224.0.0.0 - 239.255.255.255 | 0.0.0.0 |
| source-addr <src_ipv4> | Enter the source IP address. | 0.0.0.0 |

ospf

Use this command to configure Open Shortest Path First (OSPF) protocol settings on the FortiGate unit. More information on OSPF can be found in RFC 2328.

OSPF is a link state protocol capable of routing larger networks than the simpler distance vector RIP protocol. An OSPF autonomous system (AS) or routing domain is a group of areas connected to a backbone area. A router connected to more than one area is an area border router (ABR). Routing information is contained in a link state database. Routing information is communicated between routers using link state advertisements (LSAs).

Bi-directional Forwarding Detection (BFD) is a protocol used by BGP and OSPF. It is used to quickly locate hardware failures in the network. Routers running BFD communicate with each other, and if a timer runs out on a connection then that router is declared down. BFD then communicates this information to the routing protocol and the routing information is updated. BFD support can only be configured through the CLI.

Syntax

```
config router ospf
    set abr-type {cisco | ibm | shortcut | standard}
    set auto-cost-ref-bandwidth <mbps_integer>
    set bfd {enable | disable | global}
    set database-overflow {enable | disable}
    set database-overflow-max-lsas <lsas_integer>
    set database-overflow-time-to-recover <seconds_integer>
    set default-information-metric <metric_integer>
    set default-information-metric-type {1 | 2}
    set default-information-originate {always | disable | enable}
    set default-information-route-map <name_str>
    set default-metric <metric_integer>
    set distance <distance_integer>
    set distance-external <distance_integer>
    set distance-inter-area <distance_integer>
    set distance-intra-area <distance_integer>
    set distribute-list-in <access_list_name>
    set passive-interface <name_str>
    set restart-mode {graceful-restart | lls | none}
    set restart-period
    set rfc1583-compatible {enable | disable}
    set router-id <address_ipv4>
    set spf-timers <delay_integer> <hold_integer>
config area
    edit <area_address_ipv4>
        set authentication {md5 | none | text}
        set default-cost <cost_integer>
        set nssa-default-information-originate {enable | disable}
        set nssa-default-information-originate-metric <metric>
        set nssa-default-information-originate-metric-type {1 | 2}
        set nssa-redistribution {enable | disable}
        set nssa-translator-role {always | candidate | never}
        set shortcut {default | disable | enable}
```

```
set stub-type {no-summary | summary}
set type {nssa | regular | stub}
config filter-list
    edit <filter-list_id>
        set direction {in | out}
        set list <name_str>
    end
config range
    edit <range_id>
        set advertise {enable | disable}
        set prefix <address_ipv4mask>
        set substitute <address_ipv4mask>
        set substitute-status {enable | disable}
    end
config virtual-link
    edit <vlink_name>
        set authentication {md5 | none | text}
        set authentication-key <password_str>
        set dead-interval <seconds_integer>
        set hello-interval <seconds_integer>
        set md5-key <id_integer><key_str>
        set peer <address_ipv4>
        set retransmit-interval <seconds_integer>
        set transmit-delay <seconds_integer>
    end
end
config distribute-list
    edit <distribute-list_id>
        set access-list <name_str>
        set protocol {connected | rip | static}
    end
end
config neighbor
    edit <neighbor_id>
        set cost <cost_integer>
        set ip <address_ipv4>
        set poll-interval <seconds_integer>
        set priority <priority_integer>
    end
end
config network
    edit <network_id>
        set area <id-address_ipv4>
        set prefix <address_ipv4mask>
    end
end
```

```
config ospf-interface
  edit <ospf_interface_name>
    set authentication {md5 | none | text}
    set authentication-key <password_str>
    set cost <cost_integer>
    set database-filter-out {enable | disable}
    set dead-interval <seconds_integer>
    set hello-interval <seconds_integer>
    set interface <name_str>
    set ip <address_ipv4>
    set md5-key <id_integer> <key_str>
    set mtu <mtu_integer>
    set mtu-ignore {enable | disable}
    set network-type <type>
    set prefix-length <int>
    set priority <priority_integer>
    set resync-timeout <integer>
    set retransmit-interval <seconds_integer>
    set status {enable | disable}
    set transmit-delay <seconds_integer>
  end
end
config redistribute {bgp | connected | static | rip}
  set metric <metric_integer>
  set metric-type {1 | 2}
  set routemap <name_str>
  set status {enable | disable}
  set tag <tag_integer>
end
config summary-address
  edit <summary-address_id>
    set advertise {enable | disable}
    set prefix <address_ipv4mask>
    set tag <tag_integer>
  end
end
end
```

config router ospf

Use this command to set the router ID of the FortiGate unit. Additional configuration options are supported.

The `router-id` field is required. All other fields are optional.

| Variable | Description | Default |
|--|---|----------|
| abr-type { cisco ibm shortcut standard } | Specify the behavior of a FortiGate unit acting as an OSPF area border router (ABR) when it has multiple attached areas and has no backbone connection. Selecting the ABR type compatible with the routers on your network can reduce or eliminate the need for configuring and maintaining virtual links. For more information, see RFC 3509. | standard |
| auto-cost-ref-bandwidth <mbps_integer> | Enter the Mbits per second for the reference bandwidth. Values can range from 1 to 65535. | 1000 |
| bfd { enable disable global } | Select one of the Bidirectional Forwarding Detection (BFD) options for this interface. <ul style="list-style-type: none"> enable - start BFD on this interface disable - stop BFD on this interface global - use the global settings instead of explicitly setting BFD per interface. For the global settings see “ system bfd {enable disable} ” on page 672. | disable |
| database-overflow { enable disable } | Enable or disable dynamically limiting link state database size under overflow conditions. Enable this command for FortiGate units on a network with routers that may not be able to maintain a complete link state database because of limited resources. | disable |
| database-overflow-max-lsas <lsas_integer> | If you have enabled <code>database-overflow</code> , set the limit for the number of external link state advertisements (LSAs) that the FortiGate unit can keep in its link state database before entering the overflow state. The <code>lsas_integer</code> must be the same on all routers attached to the OSPF area and the OSPF backbone. The valid range for <code>lsas_integer</code> is 0 to 4294967294. | 10000 |
| database-overflow-time-to-recover <seconds_integer> | Enter the time, in seconds, after which the FortiGate unit will attempt to leave the overflow state. If <code>seconds_integer</code> is set to 0, the FortiGate unit will not leave the overflow state until restarted. The valid range for <code>seconds_integer</code> is 0 to 65535. | 300 |
| default-information-metric <metric_integer> | Specify the metric for the default route set by the <code>default-information-originate</code> command. The valid range for <code>metric_integer</code> is 1 to 16777214. | 10 |

| Variable | Description | Default |
|---|---|-------------|
| default-information-metric-type { 1 2 } | Specify the OSPF external metric type for the default route set by the <code>default-information-originate</code> command. | 2 |
| default-information-originate { always disable enable } | Enter <code>enable</code> to advertise a default route into an OSPF routing domain. Use <code>always</code> to advertise a default route even if the FortiGate unit does not have a default route in its routing table. | disable |
| default-information-route-map <name_str> | If you have set <code>default-information-originate</code> to <code>always</code> , and there is no default route in the routing table, you can configure a route map to define the parameters that OSPF uses to advertise the default route. | Null |
| default-metric <metric_integer> | Specify the default metric that OSPF should use for redistributed routes. The valid range for <code>metric_integer</code> is 1 to 16777214. | 10 |
| distance <distance_integer> | Configure the administrative distance for all OSPF routes. Using administrative distance you can specify the relative priorities of different routes to the same destination. A lower administrative distance indicates a more preferred route. The valid range for <code>distance_integer</code> is 1 to 255. | 110 |
| distance-external <distance_integer> | Change the administrative distance of all external OSPF routes. The range is from 1 to 255. | 110 |
| distance-inter-area <distance_integer> | Change the administrative distance of all inter-area OSPF routes. The range is from 1 to 255. | 110 |
| distance-intra-area <distance_integer> | Change the administrative distance of all intra-area OSPF routes. The range is from 1 to 255. | 110 |
| distribute-list-in <access_list_name> | Limit route updates from the OSPF neighbor based on the Network Layer Reachability Information (NLRI) defined in the specified access list. You must create the access list before it can be selected here. See “router access-list, access-list6” on page 342 . | Null |
| passive-interface <name_str> | OSPF routing information is not sent or received through the specified interface. | No default. |
| restart-mode { graceful-restart lls none } | Select the restart mode from: <ul style="list-style-type: none"> graceful-restart - (also known as hitless restart) when FortiGate unit goes down it advertises to neighbors how long it will be down to reduce traffic lls - Enable Link-local Signaling (LLS) mode none - hitless restart (graceful restart) is disabled | none |
| restart-period <time_int> | Enter the time in seconds the restart is expected to take. | 120 |

| Variable | Description | Default |
|--|--|---------|
| rfc1583-compatible {enable disable} | Enable or disable RFC 1583 compatibility. RFC 1583 compatibility should be enabled only when there is another OSPF router in the network that only supports RFC 1583. When RFC 1583 compatibility is enabled, routers choose the path with the lowest cost. Otherwise, routers choose the lowest cost intra-area path through a non-backbone area. | disable |
| router-id <address_ipv4> | Set the router ID. The router ID is a unique number, in IP address dotted decimal format, that is used to identify an OSPF router to other OSPF routers within an area. The router ID should not be changed while OSPF is running. A router ID of 0.0.0.0 is not allowed. | 0.0.0.0 |
| spf-timers <delay_integer> <hold_integer> | Change the default shortest path first (SPF) calculation delay time and frequency. The <code>delay_integer</code> is the time, in seconds, between when OSPF receives information that will require an SPF calculation and when it starts an SPF calculation. The valid range for <code>delay_integer</code> is 0 to 4294967295. The <code>hold_integer</code> is the minimum time, in seconds, between consecutive SPF calculations. The valid range for <code>hold_integer</code> is 0 to 4294967295. OSPF updates routes more quickly if the SPF timers are set low; however, this uses more CPU. A setting of 0 for <code>spf-timers</code> can quickly use up all available CPU. | 5 10 |

Example

This example shows how to set the OSPF router ID to 1.1.1.1 for a standard area border router:

```
config router ospf
    set abr-type standard
    set router-id 1.1.1.1
end
```

config area

Use this subcommand to set OSPF area related parameters. Routers in an OSPF autonomous system (AS) or routing domain are organized into logical groupings called areas. Areas are linked together by area border routers (ABRs). There must be a backbone area that all areas can connect to. You can use a virtual link to connect areas that do not have a physical connection to the backbone. Routers within an OSPF area maintain link state databases for their own areas.

FortiGate units support the three main types of areas—stub areas, Not So Stubby areas (NSSA), and regular areas. A stub area only has a default route to the rest of the OSPF routing domain. NSSA is a type of stub area that can import AS external routes and send them to the backbone, but cannot receive AS external routes from the backbone or other areas. All other areas are considered regular areas.

You can use the `config filter-list` subcommand to control the import and export of LSAs into and out of an area. For more information, see [“config filter-list variables” on page 400](#).

You can use access or prefix lists for OSPF area filter lists. For more information, see [“router access-list, access-list6” on page 342](#) and [“router prefix-list, prefix-list6” on page 421](#).

You can use the `config range` subcommand to summarize routes at an area boundary. If the network numbers in an area are contiguous, the ABR advertises a summary route that includes all the networks within the area that are within the specified range. See [“config range variables” on page 400](#).

You can configure a virtual link using the `config virtual-link` subcommand to connect an area to the backbone when the area has no direct connection to the backbone (see [“config virtual-link variables” on page 401](#)). A virtual link allows traffic from the area to transit a directly connected area to reach the backbone. The transit area cannot be a stub area. Virtual links can only be set up between two ABRs.



If you define a filter list, the `direction` and `list` fields are required. If you define a range, the `prefix` field is required. If you define a virtual link, the `peer` field is required. All other fields are optional.

If you configure authentication for interfaces, the authentication configured for the area is overridden.

| Variable | Description | Default |
|---|--|-------------|
| <code>edit <area_address_ipv4></code> | Type the IP address of the area. An address of 0.0.0.0 indicates the backbone area. | No default. |
| <code>authentication { md5 none text }</code> | Define the authentication used for OSPF packets sent and received in this area. Choose one of: none — no authentication is used. text — the authentication key is sent as plain text. md5 — the authentication key is used to generate an MD5 hash. Both text mode and MD5 mode only guarantee the authenticity of the OSPF packet, not the confidentiality of the information in the packet. In text mode the key is sent in clear text over the network, and is only used to prevent network problems that can occur if a misconfigured router is mistakenly added to the area. Authentication passwords or keys are defined per interface. For more information, see “config ospf-interface” on page 405 . | none |
| <code>default-cost <cost_integer></code> | Enter the metric to use for the summary default route in a stub area or not so stubby area (NSSA). A lower default cost indicates a more preferred route. The valid range for <code>cost_integer</code> is 1 to 16777214. | 10 |
| <code>nssa-default-information-originate { enable disable }</code> | Enter <code>enable</code> to advertise a default route in a not so stubby area. Affects NSSA ABRs or NSSA Autonomous System Boundary Routers only. | disable |
| <code>nssa-default-information-originate-metric <metric></code> | Specify the metric (an integer) for the default route set by the <code>nssa-default-information-originate</code> field. | 10 |

| Variable | Description | Default |
|---|--|--------------------|
| nssa-default-information-originate-metric-type {1 2} | Specify the OSPF external metric type for the default route set by the <code>nssa-default-information-originate</code> field. | 2 |
| nssa-redistribution {enable disable} | Enable or disable redistributing routes into a NSSA area. | enable |
| nssa-translator-role {always candidate never} | <p>A NSSA border router can translate the Type 7 LSAs used for external route information within the NSSA to Type 5 LSAs used for distributing external route information to other parts of the OSPF routing domain. Usually a NSSA will have only one NSSA border router acting as a translator for the NSSA.</p> <p>You can set the translator role to <code>always</code> to ensure this FortiGate unit always acts as a translator if it is in a NSSA, even if other routers in the NSSA are also acting as translators.</p> <p>You can set the translator role to <code>candidate</code> to have this FortiGate unit participate in the process for electing a translator for a NSSA.</p> <p>You can set the translator role to <code>never</code> to ensure this FortiGate unit never acts as the translator if it is in a NSSA.</p> | candidate |
| shortcut {default disable enable} | Use this command to specify area shortcut parameters. | disable |
| stub-type {no-summary summary} | Enter <code>no-summary</code> to prevent an ABR sending summary LSAs into a stub area. Enter <code>summary</code> to allow an ABR to send summary LSAs into a stub area. | summary |
| type {nssa regular stub} | <p>Set the area type:</p> <ul style="list-style-type: none"> Select <code>nssa</code> for a not so stubby area. Select <code>regular</code> for a normal OSPF area. Select <code>stub</code> for a stub area. <p>This is not available for area 0.0.0.0.</p> <p>For more information, see “config area” on page 398.</p> | regular |
| config filter-list variables | | |
| edit <filter-list_id> | Enter an ID number for the filter list. The number must be an integer. | No default. |
| direction {in out} | Set the direction for the filter. Enter <code>in</code> to filter incoming packets. Enter <code>out</code> to filter outgoing packets. | out |
| list <name_str> | Enter the name of the access list or prefix list to use for this filter list. | Null. |
| config range variables | | |
| edit <range_id> | Enter an ID number for the range. The number must be an integer in the 0 to 4 294 967 295 range. | No default. |
| advertise {enable disable} | Enable or disable advertising the specified range. | enable |
| prefix <address_ipv4mask> | Specify the range of addresses to summarize. | 0.0.0.0 0.0.0.0 |
| substitute <address_ipv4mask> | Enter a prefix to advertise instead of the prefix defined for the range. The prefix 0.0.0.0 0.0.0.0 is not allowed. | 0.0.0.0 0.0.0.0 |

| Variable | Description | Default |
|---------------------------------------|---|--------------------|
| substitute-status {enable disable} | Enable or disable using a substitute prefix. | disable |
| config virtual-link variables | | |
| edit <vlink_name> | Enter a name for the virtual link. | No default. |
| authentication {md5 none text} | <p>Define the type of authentication used for OSPF packets sent and received over this virtual link. Choose one of:</p> <p>none — no authentication is used.</p> <p>text — the authentication key is sent as plain text.</p> <p>md5 — the authentication key is used to generate an MD5 hash.</p> <p>Both text mode and MD5 mode only guarantee the authenticity of the OSPF packet, not the confidentiality of the information in the packet.</p> <p>In text mode the key is sent in clear text over the network, and is only used only to prevent network problems that can occur if a misconfigured router is mistakenly added to the area.</p> | none |
| authentication-key <password_str> | <p>Enter the password to use for <code>text</code> authentication. The maximum length for the <code>authentication-key</code> is 15 characters.</p> <p>The <code>authentication-key</code> used must be the same on both ends of the virtual link.</p> <p>This field is only available when <code>authentication</code> is set to <code>text</code>.</p> | * (No default.) |
| dead-interval <seconds_integer> | <p>The time in seconds to wait for a hello packet before declaring a router down. The value of the <code>dead-interval</code> should be four times the value of the <code>hello-interval</code>.</p> <p>Both ends of the virtual link must use the same value for <code>dead-interval</code>.</p> <p>The valid range for <code>seconds_integer</code> is 1 to 65535.</p> | 40 |
| hello-interval <seconds_integer> | <p>The time, in seconds, between hello packets.</p> <p>Both ends of the virtual link must use the same value for <code>hello-interval</code>.</p> <p>The value for <code>dead-interval</code> should be four times larger than the <code>hello-interval</code> value.</p> <p>The valid range for <code>seconds_integer</code> is 1 to 65535.</p> | 10 |

| Variable | Description | Default |
|--|--|-------------|
| md5-key <id_integer><key_str> | <p>This field is available when authentication is set to md5.</p> <p>Enter the key ID and password to use for MD5 authentication. Example:</p> <pre>set md5-key 6 "ENC yYKaPSrY89CeXn66WUybbLZQ5YM="</pre> <p>Both ends of the virtual link must use the same key ID and key.</p> <p>The valid range for <code>id_integer</code> is 1 to 255. <code>key_str</code> is an alphanumeric string of up to 16 characters.</p> | No default. |
| peer <address_ipv4> | <p>The router id of the remote ABR.</p> <p>0.0.0.0 is not allowed.</p> | 0.0.0.0 |
| retransmit-interval <seconds_integer> | <p>The time, in seconds, to wait before sending a LSA retransmission. The value for the retransmit interval must be greater than the expected round-trip delay for a packet. The valid range for <code>seconds_integer</code> is 1 to 65535.</p> | 5 |
| transmit-delay <seconds_integer> | <p>The estimated time, in seconds, required to send a link state update packet on this virtual link.</p> <p>OSPF increments the age of the LSAs in the update packet to account for transmission and propagation delays on the virtual link.</p> <p>Increase the value for <code>transmit-delay</code> on low speed links.</p> <p>The valid range for <code>seconds_integer</code> is 1 to 65535.</p> | 1 |

Example

This example shows how to configure a stub area with the id 15.1.1.1, a stub type of `summary`, a default cost of 20, and MD5 authentication.

```
config router ospf
  config area
    edit 15.1.1.1
      set type stub
      set stub-type summary
      set default-cost 20
      set authentication md5
    end
  end
```

This example shows how to use a filter list named `acc_list1` to filter packets entering area 15.1.1.1.

```
config router ospf
  config area
    edit 15.1.1.1
      config filter-list
        edit 1
          set direction in
          set list acc_list1
        end
      end
    end
```

This example shows how to set the prefix for range 1 of area 15.1.1.1.

```
config router ospf
  config area
    edit 15.1.1.1
      config range
        edit 1
          set prefix 1.1.0.0 255.255.0.0
        end
      end
    end
```

This example shows how to configure a virtual link.

```
config router ospf
  config area
    edit 15.1.1.1
      config virtual-link
        edit vlnk1
          set peer 1.1.1.1
        end
      end
    end
```

config distribute-list

Use this subcommand to filter the networks for routing updates using an access list. Routes not matched by any of the distribution lists will not be advertised.

You must configure the access list that you want the distribution list to use before you configure the distribution list. To configure an access list, see [“router access-list, access-list6” on page 342](#).

The `access-list` and `protocol` fields are required.

| Variable | Description | Default |
|--|---|-------------|
| edit <distribute-list_id> | Enter an ID number for the distribution list. The number must be an integer. | No default. |
| access-list <name_str> | Enter the name of the access list to use for this distribution list. | Null |
| protocol {connected rip static} | Advertise only the routes discovered by the specified protocol and that are permitted by the named access list. | connected |

Example

This example shows how to configure distribution list 2 to use an access list named `acc_list1` for all static routes.

```
config router ospf
  config distribute-list
    edit 2
      set access-list acc_list1
      set protocol static
    end
  end
```

config neighbor

Use this subcommand to manually configure an OSPF neighbor on non-broadcast networks. OSPF packets are unicast to the specified neighbor address. You can configure multiple neighbors.

The `ip` field is required. All other fields are optional.

| Variable | Description | Default |
|------------------------------------|---|-------------|
| edit <neighbor_id> | Enter an ID number for the OSPF neighbor. The number must be an integer. | No default. |
| cost <cost_integer> | Enter the cost to use for this neighbor. The valid range for <code>cost_integer</code> is 1 to 65535. | 10 |
| ip <address_ipv4> | Enter the IP address of the neighbor. | 0.0.0.0 |
| poll-interval <seconds_integer> | Enter the time, in seconds, between hello packets sent to the neighbor in the down state. The value of the poll interval must be larger than the value of the hello interval. The valid range for <code>seconds_integer</code> is 1 to 65535. | 10 |
| priority <priority_integer> | Enter a priority number for the neighbor. The valid range for <code>priority_integer</code> is 0 to 255. | 1 |

Example

This example shows how to manually add a neighbor.

```
config router ospf
  config neighbor
    edit 1
      set ip 192.168.21.63
    end
  end
```

config network

Use this subcommand to identify the interfaces to include in the specified OSPF area. The `prefix` field can define one or multiple interfaces.

The `area` and `prefix` fields are required.

| Variable | Description | Default |
|--|--|--------------------|
| <code>edit <network_id></code> | Enter an ID number for the network. The number must be an integer. | No default. |
| <code>area <id-address_ipv4></code> | The ID number of the area to be associated with the prefix. | 0.0.0.0 |
| <code>prefix <address_ipv4mask></code> | Enter the IP address and netmask for the OSPF network. | 0.0.0.0 0.0.0.0 |

Example

Use the following command to enable OSPF for the interfaces attached to networks specified by the IP address 10.0.0.0 and the netmask 255.255.255.0 and to add these interfaces to area 10.1.1.1.

```
config router ospf
  config network
    edit 2
      set area 10.1.1.1
      set prefix 10.0.0.0 255.255.255.0
    end
  end
```

config ospf-interface

Use this subcommand to configure interface related OSPF settings.



The `interface` field is required. All other fields are optional.

If you configure authentication for the interface, authentication for areas is not used.

| Variable | Description | Default |
|---|---|-------------|
| <code>edit <ospf_interface_name></code> | Enter a descriptive name for this OSPF interface configuration. To apply this configuration to a FortiGate unit interface, set the <code>interface <name_str></code> attribute. | No default. |

| Variable | Description | Default |
|---|--|-------------|
| authentication {md5 none text} | <p>Define the authentication used for OSPF packets sent and received by this interface. Choose one of:</p> <p>none — no authentication is used.</p> <p>text — the authentication key is sent as plain text.</p> <p>md5 — the authentication key is used to generate an MD5 hash.</p> <p>Both text mode and MD5 mode only guarantee the authenticity of the update packet, not the confidentiality of the routing information in the packet.</p> <p>In text mode the key is sent in clear text over the network, and is only used only to prevent network problems that can occur if a misconfigured router is mistakenly added to the network.</p> <p>All routers on the network must use the same authentication type.</p> | none |
| authentication-key <password_str> | <p>This field is available when <code>authentication</code> is set to <code>text</code>.</p> <p>Enter the password to use for <code>text</code> authentication.</p> <p>The <code>authentication-key</code> must be the same on all neighboring routers.</p> <p>The maximum length for the <code>authentication-key</code> is 15 characters.</p> | No default. |
| bfd {enable disable} | <p>Select to enable Bi-directional Forwarding Detection (BFD). It is used to quickly detect hardware problems on the network.</p> <p>This command enables this service on this interface.</p> | |
| cost <cost_integer> | Specify the cost (metric) of the link. The cost is used for shortest path first calculations. | 10 |
| database-filter-out {enable disable} | Enable or disable flooding LSAs out of this interface. | disable |
| dead-interval <seconds_integer> | <p>The time, in seconds, to wait for a hello packet before declaring a router down. The value of the <code>dead-interval</code> should be four times the value of the <code>hello-interval</code>.</p> <p>All routers on the network must use the same value for <code>dead-interval</code>.</p> <p>The valid range for <code>seconds_integer</code> is 1 to 65535.</p> | 40 |
| hello-interval <seconds_integer> | <p>The time, in seconds, between hello packets.</p> <p>All routers on the network must use the same value for <code>hello-interval</code>.</p> <p>The value of the <code>dead-interval</code> should be four times the value of the <code>hello-interval</code>.</p> <p>The valid range for <code>seconds_integer</code> is 1 to 65535.</p> | 10 |
| interface <name_str> | Enter the name of the interface to associate with this OSPF configuration. The interface might be a virtual IPsec or GRE interface. | Null. |

| Variable | Description | Default |
|-----------------------------------|---|-------------|
| ip <address_ipv4> | <p>Enter the IP address of the interface named by the <code>interface</code> field.</p> <p>It is possible to apply different OSPF configurations for different IP addresses defined on the same interface.</p> | 0.0.0.0 |
| md5-key <id_integer> <key_str> | <p>This field is available when authentication is set to md5.</p> <p>Enter the key ID and password to use for MD5 authentication. Example:</p> <pre>set md5-key 6 "ENC yYKaPSrY89CeXn66WUybbLZQ5YM="</pre> <p>You can add more than one key ID and key pair per interface. However, you cannot unset one key without unsetting all of the keys.</p> <p>The key ID and key must be the same on all neighboring routers.</p> <p>The valid range for <code>id_integer</code> is 1 to 255. <code>key_str</code> is an alphanumeric string of up to 16 characters.</p> | No default. |
| mtu <mtu_integer> | Change the Maximum Transmission Unit (MTU) size included in database description packets sent out this interface. The valid range for <code>mtu_integer</code> is 576 to 65535. | 1500 |
| mtu-ignore {enable disable} | <p>Use this command to control the way OSPF behaves when the Maximum Transmission Unit (MTU) in the sent and received database description packets does not match.</p> <p>When <code>mtu-ignore</code> is enabled, OSPF will stop detecting mismatched MTUs and go ahead and form an adjacency.</p> <p>When <code>mtu-ignore</code> is disabled, OSPF will detect mismatched MTUs and not form an adjacency.</p> <p><code>mtu-ignore</code> should only be enabled if it is not possible to reconfigure the MTUs so that they match on both ends of the attempted adjacency connection.</p> | disable |
| network-type <type> | <p>Specify the type of network to which the interface is connected.</p> <p>OSPF supports four different types of network. This command specifies the behavior of the OSPF interface according to the network type. Choose one of:</p> <p>broadcast</p> <p>non-broadcast</p> <p>point-to-multipoint</p> <p>point-to-multipoint-non-broadcast</p> <p>point-to-point</p> <p>If you specify <code>non-broadcast</code>, you must also configure neighbors using “config neighbor” on page 404.</p> | broadcast |
| prefix-length <int> | Set the size of the OSPF hello network mask. Range 0 to 32. | 0 |

| Variable | Description | Default |
|--|---|---------|
| priority <priority_integer> | <p>Set the router priority for this interface.</p> <p>Router priority is used during the election of a designated router (DR) and backup designated router (BDR).</p> <p>An interface with router priority set to 0 can not be elected DR or BDR. The interface with the highest router priority wins the election. If there is a tie for router priority, router ID is used.</p> <p>Point-to-point networks do not elect a DR or BDR; therefore, this setting has no effect on a point-to-point network.</p> <p>The valid range for <code>priority_integer</code> is 0 to 255.</p> | 1 |
| resync-timeout <integer> | Enter the synchronizing timeout for graceful restart interval in seconds. This is the period for this interface to synchronize with a neighbor. | 40 |
| retransmit-interval <seconds_integer> | The time, in seconds, to wait before sending a LSA retransmission. The value for the retransmit interval must be greater than the expected round-trip delay for a packet. The valid range for <code>seconds_integer</code> is 1 to 65535. | 5 |
| status {enable disable} | Enable or disable OSPF on this interface. | enable |
| transmit-delay <seconds_integer> | <p>The estimated time, in seconds, required to send a link state update packet on this interface.</p> <p>OSPF increments the age of the LSAs in the update packet to account for transmission and propagation delays on the interface.</p> <p>Increase the value for <code>transmit-delay</code> on low speed links.</p> <p>The valid range for <code>seconds_integer</code> is 1 to 65535.</p> | 1 |

Example

This example shows how to assign an OSPF interface configuration named `test` to the interface named `internal` and how to configure text authentication for this interface.

```

config router ospf
  config ospf-interface
    edit test
      set interface internal
      set ip 192.168.20.3
      set authentication text
      set authentication-key a2b3c4d5e
    end
  end
end

```


config redistribute

Use this subcommand to redistribute routes learned from BGP, RIP, static routes, or a direct connection to the destination network.

The OSPF redistribution table contains four static entries. You cannot add entries to the table. The entries are defined as follows:

- `bgp` — Redistribute routes learned from BGP.
- `connected` — Redistribute routes learned from a direct connection to the destination network.
- `isis` — Redistribute routes learned from ISIS.
- `static` — Redistribute the static routes defined in the FortiGate unit routing table.
- `rip` — Redistribute routes learned from RIP.

When you enter the subcommand, end the command with one of the four static entry names (that is, `config redistribute {bgp | connected | isis | static | rip}`).

All fields are optional.

| Variable | Description | Default |
|--|---|---------|
| <code>metric <metric_integer></code> | Enter the metric to be used for the redistributed routes. The <code>metric_integer</code> range is from 1 to 16777214. | 10 |
| <code>metric-type {1 2}</code> | Specify the external link type to be used for the redistributed routes. | 2 |
| <code>routemap <name_str></code> | Enter the name of the route map to use for the redistributed routes. For information on how to configure route maps, see “router route-map” on page 438 . | Null |
| <code>status {enable disable}</code> | Enable or disable redistributing routes. | disable |
| <code>tag <tag_integer></code> | Specify a tag for redistributed routes. The valid range for <code>tag_integer</code> is 0 to 4294967295. | 0 |

Example

This example shows how to enable route redistribution from RIP, using a metric of 3 and a route map named `rtmp2`.

```
config router ospf
  config redistribute rip
    set metric 3
    set routemap rtmp2
    set status enable
  end
```

config summary-address

Use this subcommand to summarize external routes for redistribution into OSPF. This command works only for summarizing external routes on an Autonomous System Boundary Router (ASBR). For information on summarization between areas, see [“config range variables” on page 400](#). By replacing the LSAs for each route with one aggregate route, you reduce the size of the OSPF link-state database.

The `prefix` field is required. All other fields are optional.

| Variable | Description | Default |
|------------------------------|--|--------------------|
| edit <summary-address_id> | Enter an ID number for the summary address. The number must be an integer. | No default. |
| advertise {enable disable} | Advertise or suppress the summary route that matches the specified prefix. | enable |
| prefix <address_ipv4mask> | Enter the prefix (IP address and netmask) to use for the summary route. The prefix 0.0.0.0 0.0.0.0 is not allowed. | 0.0.0.0 0.0.0.0 |
| tag <tag_integer> | Specify a tag for the summary route. The valid range for <code>tag_integer</code> is 0 to 4294967295. | 0 |

ospf6

Use this command to configure OSPF routing for IPv6 traffic.

IP version 6 for OSPF is supported through Open Shortest Path First version 3 (OSPFv3) defined in RFC 2740. This includes the Authentication/Confidentiality for OSPFv3.

For more information on OSPF features in general, see “[config router ospf](#)” on page 396.

Syntax

```
config router ospf6
    set abr-type {cisco | ibm | standard}
    set auto-cost-ref-bandwidth <mbps_integer>
    set default-metric <metric_integer>
    set passive-interface <name_str>
    set router-id <address_ipv6>
    set spf-timers <delay_integer> <hold_integer>
    config area
        edit <area_address_ipv6>
            set default-cost <cost_integer>
            set nssa-default-information-originate {enable | disable}
            set nssa-default-information-originate-metric <metric>
            set nssa-default-information-originate-metric-type {1 | 2}
            set nssa-redistribution {enable | disable}
            set nssa-translator-role {always | candidate | never}
            set stub-type {no-summary | summary}
            set type {regular | stub | nssa}
        end
    config ospf6-interface
        edit <ospf6_interface_name>
            set area-id <ip4_addr>
            set cost <cost_integer>
            set dead-interval <seconds_integer>
            set hello-interval <seconds_integer>
            set interface <name_str>
            set network-type <type_str>
            set priority <priority_integer>
            set retransmit-interval <seconds_integer>
            set status {enable | disable}
            set transmit-delay <seconds_integer>
            config neighbor
                edit <neighbor_addr>
                    set cost <cost_integer>
                    set poll-interval <seconds_integer>
                    set priority <priority_integer>
                end
            end
        end
    end
```

```

config redistribute {bgp | connected | rip | static}
  set metric <metric_integer>
  set metric-type {1 | 2}
  set routemap <name_str>
  set status {enable | disable}
end
end

```

| Variable | Description | Default |
|--|--|-------------|
| abr-type {cisco ibm standard} | Specify the behavior of a FortiGate unit acting as an OSPF area border router (ABR) when it has multiple attached areas and has no backbone connection. Selecting the ABR type compatible with the routers on your network can reduce or eliminate the need for configuring and maintaining virtual links. For more information, see RFC 3509. | standard |
| auto-cost-ref-bandwidth <mbps_integer> | Enter the Mbits per second for the reference bandwidth. Values can range from 1 to 65535. | 1000 |
| default-metric <metric_integer> | Specify the default metric that OSPF should use for redistributed routes. The valid range for <code>metric_integer</code> is 1 to 16777214. | 10 |
| passive-interface <name_str> | OSPF routing information is not sent or received through the specified interface. | No default. |
| router-id <address_ipv6> | Set the router ID. The router ID is a unique number, in IP address dotted decimal format, that is used to identify an OSPF router to other OSPF routers within an area. The router ID should not be changed while OSPF is running. A router ID of 0.0.0.0 is not allowed. | :: |
| spf-timers <delay_integer> <hold_integer> | Change the default shortest path first (SPF) calculation delay time and frequency. The <code>delay_integer</code> is the time, in seconds, between when OSPF receives information that will require an SPF calculation and when it starts an SPF calculation. The valid range for <code>delay_integer</code> is 0 to 4294967295. The <code>hold_integer</code> is the minimum time, in seconds, between consecutive SPF calculations. The valid range for <code>hold_integer</code> is 0 to 4294967295. OSPF updates routes more quickly if the SPF timers are set low; however, this uses more CPU. A setting of 0 for <code>spf-timers</code> can quickly use up all available CPU. | 5 10 |

config area

Use this subcommand to set OSPF area related parameters. Routers in an OSPF autonomous system (AS) or routing domain are organized into logical groupings called areas. Areas are linked together by area border routers (ABRs). There must be a backbone area that all areas can connect to. You can use a virtual link to connect areas that do not have a physical connection to the backbone. Routers within an OSPF area maintain link state databases for their own areas.

You can use the `config range` subcommand to summarize routes at an area boundary. If the network numbers in an area are contiguous, the ABR advertises a summary route that includes all the networks within the area that are within the specified range. See [“config range variables” on page 400](#).

You can configure a virtual link using the `config virtual-link` subcommand to connect an area to the backbone when the area has no direct connection to the backbone (see [“config virtual-link variables” on page 401](#)). A virtual link allows traffic from the area to transit a directly connected area to reach the backbone. The transit area cannot be a stub area. Virtual links can only be set up between two ABRs.

| Variable | Description | Default |
|--|---|-------------|
| <code>edit</code> <code><area_address_ipv6></code> | Type the IP address of the area. An address of <code>::</code> indicates the backbone area. | No default. |
| <code>default-cost</code> <code><cost_integer></code> | Enter the metric to use for the summary default route in a stub area or not so stubby area (NSSA). A lower default cost indicates a more preferred route. The valid range for <code>cost_integer</code> is 1 to 16777214. | 10 |
| <code>nssa-default-information-originate</code> { <code>enable</code> <code>disable</code> } | Enter <code>enable</code> to advertise a default route in a not so stubby area. Affects NSSA ABRs or NSSA Autonomous System Boundary Routers only. | disable |
| <code>nssa-default-information-originate-metric</code> <code><metric></code> | Specify the metric (an integer) for the default route set by the <code>nssa-default-information-originate</code> field. Range 0-16 777 214. | 10 |
| <code>nssa-default-information-originate-metric-type</code> {1 2} | Specify the OSPF external metric type for the default route set by the <code>nssa-default-information-originate</code> field. | 2 |
| <code>nssa-redistribution</code> { <code>enable</code> <code>disable</code> } | Enable or disable redistributing routes into a NSSA area. | enable |
| <code>nssa-translator-role</code> { <code>always</code> <code>candidate</code> <code>never</code> } | A NSSA border router can translate the Type 7 LSAs used for external route information within the NSSA to Type 5 LSAs used for distributing external route information to other parts of the OSPF routing domain. Usually a NSSA will have only one NSSA border router acting as a translator for the NSSA. You can set the translator role to <code>always</code> to ensure this FortiGate unit always acts as a translator if it is in a NSSA, even if other routers in the NSSA are also acting as translators. You can set the translator role to <code>candidate</code> to have this FortiGate unit participate in the process for electing a translator for a NSSA. You can set the translator role to <code>never</code> to ensure this FortiGate unit never acts as the translator if it is in a NSSA. | candidate |
| <code>stub-type</code> { <code>no-summary</code> <code>summary</code> } | Select the type of communication with the stub area. Choose one of: no-summary — prevent an ABR sending summary LSAs into a stub area. summary — allow an ABR to send summary LSAs into a stub area. | summary |

| Variable | Description | Default |
|--|--|-------------|
| type {regular stub nssa} | For the type of area, choose one of: regular — for a normal OSPF area. stub — for a stub area that has limited connections to other areas. nssa — for a not so stubby area | regular |
| config range Variables | | |
| edit <range_id> | Enter an ID number for the range. The number must be an integer in the 0 to 4 294 967 295 range. | No default. |
| advertise {enable disable} | Enable or disable advertising the specified range. | enable |
| prefix6 <address_ipv6mask> | Specify the range of addresses to summarize. | ::/0 |
| config virtual-link Variables | | |
| edit <vlink_name> | Enter a name for the virtual link. | No default. |
| dead-interval <seconds_integer> | The time, in seconds, to wait for a hello packet before declaring a router down. The value of the dead-interval should be four times the value of the hello-interval. Both ends of the virtual link must use the same value for dead-interval. The valid range for seconds_integer is 1 to 65535. | 40 |
| hello-interval <seconds_integer> | The time, in seconds, between hello packets. Both ends of the virtual link must use the same value for hello-interval. The valid range for seconds_integer is 1 to 65535. | 10 |
| peer <address_ipv4> | The router id of the remote ABR. 0 . 0 . 0 . 0 is not allowed. | 0.0.0.0 |
| retransmit-interval <seconds_integer> | The time, in seconds, to wait before sending a LSA retransmission. The value for the retransmit interval must be greater than the expected round-trip delay for a packet. The valid range for seconds_integer is 1 to 65535. | 5 |
| transmit-delay <seconds_integer> | The estimated time, in seconds, required to send a link state update packet on this virtual link. OSPF increments the age of the LSAs in the update packet to account for transmission and propagation delays on the virtual link. Increase the value for transmit-delay on low speed links. The valid range for seconds_integer is 1 to 65535. | 1 |

config ospf6-interface

Use this subcommand to change interface related OSPF settings. The `interface` field is required. All other fields are optional.

| Variable | Description | Default |
|--|--|-------------|
| edit <ospf6_interface_name> | Enter a descriptive name for this OSPF interface configuration. To apply this configuration to a FortiGate unit interface, set the <code>interface <name_str></code> attribute. | No default. |
| area-id <ip4_addr> | Enter the area ID in A.B.C.D IPv4 format. | 0.0.0.0 |
| cost <cost_integer> | Specify the cost (metric) of the link. The cost is used for shortest path first calculations. Range 1 to 65 535. Use 0 for auto-cost. | 0 |
| dead-interval <seconds_integer> | The time, in seconds, to wait for a hello packet before declaring a router down. The value of the <code>dead-interval</code> should be four times the value of the <code>hello-interval</code> . All routers on the network must use the same value for <code>dead-interval</code> . The valid range for <code>seconds_integer</code> is 1 to 65535. | 40 |
| hello-interval <seconds_integer> | The time, in seconds, between hello packets. All routers on the network must use the same value for <code>hello-interval</code> . The valid range for <code>seconds_integer</code> is 1 to 65535. | 10 |
| interface <name_str> | Enter the name of the interface to associate with this OSPF configuration. The interface might be a virtual IPsec or GRE interface. | Null |
| network-type <type_str> | Choose the network type, one of: broadcast, non-broadcast, point-to-point, point-to-multipoint, point-to-multipoint-non-broadcast. | broadcast |
| priority <priority_integer> | Set the router priority for this interface. Router priority is used during the election of a designated router (DR) and backup designated router (BDR). An interface with router priority set to 0 can not be elected DR or BDR. The interface with the highest router priority wins the election. If there is a tie for router priority, router ID is used. Point-to-point networks do not elect a DR or BDR; therefore, this setting has no effect on a point-to-point network. The valid range for <code>priority_integer</code> is 0 to 255. | 1 |
| retransmit-interval <seconds_integer> | The time, in seconds, to wait before sending a LSA retransmission. The value for the retransmit interval must be greater than the expected round-trip delay for a packet. The valid range for <code>seconds_integer</code> is 1 to 65535. | 5 |
| status {enable disable} | Enable or disable OSPF on this interface. | enable |

| Variable | Description | Default |
|-------------------------------------|--|-------------|
| transmit-delay <seconds_integer> | The estimated time, in seconds, required to send a link state update packet on this interface. OSPF increments the age of the LSAs in the update packet to account for transmission and propagation delays on the interface. Increase the value for <code>transmit-delay</code> on low speed links. The valid range for <code>seconds_integer</code> is 1 to 65535. | 1 |
| config neighbor variables | | |
| edit <neighbor_addr> | Enter the IPv6 link local address of the neighbor. | No default. |
| cost <cost_integer> | Enter the cost to use for this neighbor. The valid range for <code>cost_integer</code> is 1 to 65535. | 10 |
| poll-interval <seconds_integer> | Enter the time, in seconds, between hello packets sent to the neighbor in the down state. The value of the poll interval must be larger than the value of the hello interval. The valid range for <code>seconds_integer</code> is 1 to 65535. | 10 |
| priority <priority_integer> | Enter a priority number for the neighbor. The valid range for <code>priority_integer</code> is 0 to 255. | 1 |

config redistribute

Use this subcommand to redistribute routes learned from BGP, RIP, static routes, or a direct connection to the destination network.

The OSPF redistribution table contains four static entries. You cannot add entries to the table. The entries are defined as follows:

- `bgp` — Redistribute routes learned from BGP.
- `connected` — Redistribute routes learned from a direct connection to the destination network.
- `isis` — Redistribute routes learned from ISIS.
- `static` — Redistribute the static routes defined in the FortiGate unit routing table.
- `rip` — Redistribute routes learned from RIP.

When you enter the subcommand, end the command with one of the four static entry names (that is, `config redistribute {bgp | connected | isis | rip | static}`).

All fields are optional.

| Variable | Description | Default |
|---------------------------|--|---------|
| metric <metric_integer> | Enter the metric to be used for the redistributed routes. The <code>metric_integer</code> range is from 1 to 16777214. | 10 |
| metric-type {1 2} | Specify the external link type to be used for the redistributed routes. | 2 |
| route-map <name_str> | Enter the name of the route map to use for the redistributed routes. | Null. |
| status {enable disable} | Enable or disable redistributing routes. | disable |

policy, policy6

Use this command to add, move, edit or delete a route policy. When you create a policy route, any packets that match the policy are forwarded to the IP address of the next-hop gateway through the specified outbound interface.

You can configure the FortiGate unit to route packets based on:

- a source address
- a protocol, service type, or port range
- the inbound interface
- type of service (TOS)

When the FortiGate unit receives a packet, it starts at the top of the policy routing list and attempts to match the packet with a policy in ascending order. If no packets match the policy route, the FortiGate unit routes the packet using the routing table. Route policies are processed before static routing. You can change the order of policy routes using the `move` command.



For static routing, any number of static routes can be defined for the same destination. When multiple routes for the same destination exist, the FortiGate unit chooses the route having the lowest administrative distance. Route redundancy is not available for policy routing: any packets that match a route policy are forwarded according to the route specified in the policy.

Type of service (TOS) is an 8-bit field in the IP header that enables you to determine how the IP datagram should be delivered, with such criteria as delay, priority, reliability, and minimum cost. Each quality helps gateways determine the best way to route datagrams. A router maintains a ToS value for each route in its routing table. The lowest priority TOS is 0, the highest is 7 - when bits 3, 4, and 5 are all set to 1. The router tries to match the TOS of the datagram to the TOS on one of the possible routes to the destination. If there is no match, the datagram is sent over a zero TOS route. Using increased quality may increase the cost of delivery because better performance may consume limited network resources. For more information see RFC 791 and RFC 1349.

Table 1: The role of each bit in the IP header TOS 8-bit field

| | | |
|---------------------|--------------------|--|
| bits 0, 1, 2 | Precedence | Some networks treat high precedence traffic as more important traffic. Precedence should only be used within a network, and can be used differently in each network. Typically you do not care about these bits. |
| bit 3 | Delay | When set to 1, this bit indicates low delay is a priority. This is useful for such services as VoIP where delays degrade the quality of the sound. |
| bit 4 | Throughput | When set to 1, this bit indicates high throughput is a priority. This is useful for services that require lots of bandwidth such as video conferencing. |
| bit 5 | Reliability | When set to 1, this bit indicates high reliability is a priority. This is useful when a service must always be available such as with DNS servers. |

Table 1: The role of each bit in the IP header TOS 8-bit field

| | | |
|--------------|--------------------------------|--|
| bit 6 | Cost | When set to 1, this bit indicates low cost is a priority. Generally there is a higher delivery cost associated with enabling bits 3,4, or 5, and bit 6 indicates to use the lowest cost route. |
| bit 7 | Reserved for future use | Not used at this time. |

The two fields `tos` and `tos-mask` enable you to configure type of service support on your FortiGate unit. `tos-mask` enables you to only look at select bits of the 8-bit TOS field in the IP header. This is useful as you may only care about reliability for some traffic, and not about the other TOS criteria.

The value in `tos` is used to match the pattern from `tos-mask`. If it matches, then the rest of the policy is applied. If the mask doesn't match, the next policy tries to match if its configured, and eventually default routing is applied if there are no other matches.



You need to use `tos-mask` to remove bits from the pattern you don't care about, or those bits will prevent a match with your `tos` pattern.

Syntax

```
config router policy, policy6
  move <seq-num1> {before | after} <seq-num2>
  edit <policy_integer>
    set dst <dest-address_ipv4mask>
    set end-port <port_integer>
    set end-source-port <port_integer>
    set gateway <address_ipv4>
    set input-device <interface-name_str>
    set output-device <interface-name_str>
    set protocol <protocol_integer>
    set src <source-address_ipv4mask>
    set start-port <port_integer>
    set start-source-port <port_integer>
    set tos <hex_mask>
    set tos-mask <hex_mask>
  end
```

Use the `router policy6` command for IPv6 policy routes. The `input-device` field is required. All other fields are optional.

| Variable | Description | Default |
|--|---|-------------|
| <code>move <seq-num1> {before after} <seq-num2></code> | Move policy <seq-num1> to before or after policy. <seq-num2>. | No default. |
| <code>edit <policy_integer></code> | Enter an ID number for the route policy. The number must be an integer. | No default. |

| Variable | Description | Default |
|---------------------------------------|--|---|
| dst <dest-address_ipv4mask> | Match packets that have this destination IP address and netmask. | IPv4: 0.0.0.0 0.0.0.0 IPv6: ::/0 |
| end-port <port_integer> | The end port number of a port range for a policy route. Match packets that have this destination port range. You must configure both the <code>start-port</code> and <code>end-port</code> fields for destination-port-range matching to take effect. To specify a range, the <code>start-port</code> value must be lower than the <code>end-port</code> value. To specify a single port, the <code>start-port</code> value must be identical to the <code>end-port</code> value. The <code>port_integer</code> range is 0 to 65 535. For protocols other than 6 (TCP), 17 (UDP), and 132 (SCTP) the port number is ignored. | 65 535 |
| end-source-port <port_integer> | Set port range for source IP. Use in combination with <code>start-source-port</code> . Available when protocol is 6 (TCP), 17 (UDP), or 132 (SCTP). | 65 535 |
| gateway <address_ipv4> | Send packets that match the policy to this next hop router. | 0.0.0.0 |
| input-device <interface-name_str> | Match packets that are received on this interface. | Null |
| output-device <interface-name_str> | Send packets that match the policy out this interface. | Null |
| protocol <protocol_integer> | To perform policy routing based on the value in the protocol field of the packet, enter the protocol number to match. The Internet Protocol Number is found in the IP packet header. RFC 5237 describes protocol numbers and you can find a list of the assigned protocol numbers here . The range is from 0 to 255. A value of 0 disables the feature. Commonly used <i>protocol</i> settings include 6 to route TCP sessions, 17 for UDP sessions, 1 for ICMP sessions, 47 for GRE sessions, and 92 for multicast sessions. For protocols other than 6 (TCP), 17 (UDP), and 132 (SCTP) the port number is ignored. | 0 |
| src <source-address_ipv4mask> | Match packets that have this source IP address and netmask. | IPv4: 0.0.0.0 0.0.0.0 IPv6: ::/0 |

| Variable | Description | Default |
|----------------------------------|--|---------|
| start-port <port_integer> | <p>The start port number of a port range for a policy route. Match packets that have this destination port range. You must configure both the <code>start-port</code> and <code>end-port</code> fields for destination-port-range matching to take effect. To specify a range, the <code>start-port</code> value must be lower than the <code>end-port</code> value. To specify a single port, the <code>start-port</code> value must be identical to the <code>end-port</code> value. The <code>port_integer</code> range is 0 to 65 535.</p> <p>For protocols other than 6 (TCP), 17 (UDP), and 132 (SCTP) the port number is ignored.</p> | 1 |
| start-source-port <port_integer> | Set port range for source IP. Use in combination with <code>end-source-port</code> . Available when <code>protocol</code> is 6 (TCP), 17 (UDP), or 132 (SCTP). | 1 |
| tos <hex_mask> | <p>The type of service (TOS) mask to match after applying the <code>tos-mask</code>. This is an 8-bit hexadecimal pattern that can be from "00" to "FF".</p> <p>The <code>tos</code> mask attempts to match the quality of service for this profile. Each bit in the mask represents a different aspect of quality. A <code>tos</code> mask of "0010" would indicate reliability is important, but with normal delay and throughput. The hex mask for this pattern would be "04".</p> | Null |
| tos-mask <hex_mask> | <p>This value determines which bits in the IP header's TOS field are significant. This is an 8-bit hexadecimal mask that can be from "00" to "FF".</p> <p>Typically, only bits 3 through 6 are used for TOS, so it is necessary to mask out the other bits. To mask out everything but bits 3 through 6, the hex mask would be "1E".</p> | Null |

prefix-list, prefix-list6

Use this command to add, edit, or delete prefix lists. A prefix list is an enhanced version of an access list that allows you to control the length of the prefix netmask. Prefix lists are called by routing protocols such as RIP or OSPF.

Each rule in a prefix list consists of a prefix (IP address and netmask), the action to take for this prefix (permit or deny), and maximum and minimum prefix length settings.

The FortiGate unit attempts to match a packet against the rules in a prefix list starting at the top of the list. If it finds a match for the prefix it takes the action specified for that prefix. If no match is found the default action is deny. A prefix-list should be used to match the default route 0.0.0.0/0.

`config router setting` uses prefix-list to filter the displayed routes. For more information, see “[setting](#)” on page 445.

Syntax

```
config router prefix-list, prefix-list6
  edit <prefix_list_name>
    set comments <string>
  config rule
    edit <prefix_rule_id>
      set action {deny | permit}
      set ge <length_integer>
      set le <length_integer>
      set prefix {<address_ipv4mask> | any}
      set prefix6 {<address_ipv6mask> | any}
    end
  end
end
```

The action and prefix fields are required. All other fields are optional.

| Variable | Description | Default |
|------------------------------|---|-------------|
| edit <prefix_list_name> | Enter a name for the prefix list. A prefix list and an access list cannot have the same name. | No default. |
| config rule variables | | |
| edit <prefix_rule_id> | Enter an entry number for the rule. The number must be an integer. | No default. |
| action {deny permit} | Set the action to take for this prefix. | permit |
| comments <string> | Enter a description of this access list entry. The description can be up to 127 characters long. | |
| ge <length_integer> | Match prefix lengths that are greater than or equal to this number. The setting for ge should be less than the setting for le. The setting for ge should be greater than the netmask set for prefix. length_integer can be any number from 0 to 32. | 0 |
| le <length_integer> | Match prefix lengths that are less than or equal to this number. The setting for le should be greater than the setting for ge. length_integer can be any number from 0 to 32. | 32 |

| Variable | Description | Default |
|---|---|--------------------|
| prefix {<address_ipv4mask> any } | Enter the prefix (IPv4 address and netmask) for this prefix list rule or enter <code>any</code> to match any prefix. The length of the netmask should be less than the setting for <code>ge</code> . If prefix is set to <code>any</code> , <code>ge</code> and <code>le</code> should not be set. This variable only available for prefix-list command. | 0.0.0.0 0.0.0.0 |
| prefix6 {<address_ipv6mask> any } | Enter the prefix (IPv6 address and netmask) for this prefix list rule or enter <code>any</code> to match any prefix. The length of the netmask should be less than the setting for <code>ge</code> . If prefix6 is set to <code>any</code> , <code>ge</code> and <code>le</code> should not be set. This variable only available for prefix-list6 command. | ::/0 |

rip

Use this command to configure the Routing Information Protocol (RIP) on the FortiGate unit. RIP is a distance-vector routing protocol intended for small, relatively homogeneous networks. RIP uses hop count as its routing metric. Each network is usually counted as one hop. The network diameter is limited to 15 hops with 16 hops.

The FortiOS implementation of RIP supports RIP version 1 (see RFC 1058) and RIP version 2 (see RFC 2453). RIP version 2 enables RIP messages to carry more information, and to support simple authentication and subnet masks.



`update_timer` cannot be larger than `timeout_timer` and `garbage_timer`. Attempts to do so will generate an error.

Syntax

```
config router rip
    set default-information-originate {enable | disable}
    set default-metric <metric_integer>
    set garbage-timer <timer_integer>
    set passive-interface <name_str>
    set timeout-timer <timer_integer>
    set update-timer <timer_integer>
    set version {1 2}
    config distance
        edit <distance_id>
            set access-list <name_str>
            set distance <distance_integer>
            set prefix <address_ipv4mask>
        end
    config distribute-list
        edit <distribute_list_id>
            set direction {in | out}
            set interface <name_str>
            set listname <access/prefix-listname_str>
            set status {enable | disable}
        end
    config interface
        edit <interface_name>
            set auth-keychain <name_str>
            set auth-mode {none | text | md5}
            set auth-string <password_str>
            set receive-version {1 2}
            set send-version {1 2}
            set send-version2-broadcast {enable | disable}
            set split-horizon {poisoned | regular}
            set split-horizon-status {enable | disable}
        end
    end
```

```

config neighbor
    edit <neighbor_id>
        set ip <address_ipv4>
    end
config network
    edit <network_id>
        set prefix <address_ipv4mask>
    end
config offset-list
    edit <offset_list_id>
        set access-list <name_str>
        set direction {in | out}
        set interface <name_str>
        set offset <metric_integer>
        set status {enable | disable}
    end
config redistribute {connected | static | ospf | bgp}
    set metric <metric_integer>
    set routemap <name_str>
    set status {enable | disable}
end

```

config router rip

Use this command to specify RIP operating parameters.

All fields are optional.

| Variable | Description | Default |
|---|--|-------------|
| default-information-originate { enable disable } | Enter enable to advertise a default static route into RIP. | disable |
| default-metric <metric_integer> | For non-default routes in the static routing table and directly connected networks the default metric is the metric that the FortiGate unit advertises to adjacent routers. This metric is added to the metrics of learned routes. The default metric can be a number from 1 to 16. | 1 |
| garbage-timer <timer_integer> | The time in seconds that must elapse after the timeout interval for a route expires, before RIP deletes the route. If RIP receives an update for the route after the timeout timer expires but before the garbage timer expires then the entry is switched back to reachable. RIP timer defaults are effective in most configurations. All routers and access servers in the network should have the same RIP timer settings. The update timer interval can not be larger than the garbage timer interval. | 120 |
| passive-interface <name_str> | Block RIP broadcasts on the specified interface. You can use “config neighbor” on page 429 and the passive interface command to allow RIP to send unicast updates to the specified neighbor while blocking broadcast updates on the specified interface. | No default. |

| Variable | Description | Default |
|----------------------------------|---|---------|
| timeout-timer <timer_integer> | <p>The time interval in seconds after which a route is declared unreachable. The route is removed from the routing table. RIP holds the route until the garbage timer expires and then deletes the route. If RIP receives an update for the route before the timeout timer expires, then the timeout-timer is restarted. If RIP receives an update for the route after the timeout timer expires but before the garbage timer expires then the entry is switched back to reachable. The value of the timeout timer should be at least three times the value of the update timer.</p> <p>RIP timer defaults are effective in most configurations. All routers and access servers in the network should have the same RIP timer settings.</p> <p>The update timer interval can not be larger than the timeout timer interval.</p> | 180 |
| update-timer <timer_integer> | <p>The time interval in seconds between RIP updates.</p> <p>RIP timer defaults are effective in most configurations. All routers and access servers in the network should have the same RIP timer settings.</p> <p>The update timer interval can not be larger than timeout or garbage timer intervals.</p> | 30 |
| version {1 2} | <p>Enable sending and receiving RIP version 1 packets, RIP version 2 packets, or both for all RIP-enabled interfaces. You can override this setting on a per interface basis using the receive-version {1 2} and send-version {1 2} fields described under “config interface” on page 427.</p> | 2 |

Example

This example shows how to enable the advertising of a default static route into RIP, enable the sending and receiving of RIP version 1 packets, and raise the preference of local routes in the static routing table (the default metric) from the default of 1 to 5 - those routes will be less preferred.

```
config router rip
    set default-information-originate enable
    set version 1
    set default-metric 5
end
```

config distance

Use this subcommand to specify an administrative distance. When different routing protocols provide multiple routes to the same destination, the administrative distance sets the priority of those routes. The lowest administrative distance indicates the preferred route.

If you specify a prefix, RIP uses the specified distance when the source IP address of a packet matches the prefix.

The `distance` field is required. All other fields are optional.

| Variable | Description | Default |
|--------------------------------|--|--------------------|
| edit <distance_id> | Enter an ID number for the distance. The number must be an integer. | No default. |
| access-list <name_str> | Enter the name of an access list. The distances associated with the routes in the access list will be modified. To create an access list, see “router access-list, access-list6” on page 342 . | Null |
| distance <distance_integer> | Enter a number from 1 to 255, to set the administrative distance. This field is required. | 0 |
| prefix <address_ipv4mask> | Optionally enter a prefix to apply the administrative distance to. | 0.0.0.0 0.0.0.0 |

Example

This example shows how to change the administrative distance to 10 for all IP addresses that match the `internal_example` access-list.

```
config router rip
  config distance
    edit 1
      set distance 10
      set access-list internal_example
    end
  end
```

config distribute-list

Use this subcommand to filter incoming or outgoing updates using an access list or a prefix list. If you do not specify an interface, the filter will be applied to all interfaces. You must configure the access list or prefix list that you want the distribution list to use before you configure the distribution list. For more information on configuring access lists and prefix lists, see [“router access-list, access-list6” on page 342](#) and [“router prefix-list, prefix-list6” on page 421](#).

The `direction` and `listname` fields are required. All other fields are optional.

| Variable | Description | Default |
|--|---|-------------|
| <code>edit <distributed_list_id></code> | Enter an ID number for the distribution list. The number must be an integer. | No default. |
| <code>direction {in out}</code> | Set the direction for the filter. Enter <code>in</code> to filter incoming packets that originate from other routers. Enter <code>out</code> to filter outgoing packets the FortiGate unit is sending to other routers. | out |
| <code>interface <name_str></code> | Enter the name of the interface to apply this distribution list to. If you do not specify an interface, this distribution list will be used for all interfaces. | Null |
| <code>listname <access/prefix-listname_str></code> | Enter the name of the access list or prefix list to use for this distribution list. The prefix or access list used must be configured before configuring the distribute-list. | Null |
| <code>status {enable disable}</code> | Enable or disable this distribution list. | disable |

Example

This example shows how to configure and enable a distribution list to use an access list named `allowed_routers` for incoming updates on the `external` interface.

```
config router rip
  config distribute-list
    edit 1
      set direction in
      set interface external
      set listname allowed_routers
      set status enable
    end
  end
```

config interface

Use this subcommand to configure RIP version 2 authentication, RIP version send and receive for the specified interface, and to configure and enable split horizon.

Authentication is only available for RIP version 2 packets sent and received by an interface. You must set `auth-mode` to `none` when `receive-version` or `send-version` are set to 1 or 1 2 (both are set to 1 by default).

A split horizon occurs when a router advertises a route it learns over the same interface it learned it on. In this case the router that gave the learned route to the last router now has two entries to get to another location. However, if the primary route fails that router tries the second route to find itself as part of the route and an infinite loop is created. A poisoned split horizon will still advertise the route on the interface it received it on, but it will mark the route as unreachable. Any unreachable routes are automatically removed from the routing table. This is also called split horizon with poison reverse.

All fields are optional.

| Variable | Description | Default |
|------------------------------------|---|-------------|
| edit <interface_name> | Type the name of the FortiGate unit interface that is linked to the RIP network. The interface might be a virtual IPsec or GRE interface. | No default. |
| auth-keychain <name_str> | Enter the name of the key chain to use for authentication for RIP version 2 packets sent and received by this interface. Use key chains when you want to configure multiple keys. For information on how to configure key chains, see “key-chain” on page 377 . | Null. |
| auth-mode { none text md5 } | Use the <code>auth-mode</code> field to define the authentication used for RIP version 2 packets sent and received by this interface. Choose one of: none — no authentication is used. text — the authentication key is sent as plain text. md5 — the authentication key is used to generate an MD5 hash. Both text mode and MD5 mode only guarantee the authenticity of the update packet, not the confidentiality of the routing information in the packet. In text mode the key is sent in clear text over the network. Text mode is usually used only to prevent network problems that can occur if an unwanted or misconfigured router is mistakenly added to the network. Use the <code>auth-string</code> field to specify the key. | none |
| auth-string <password_str> | Enter a single key to use for authentication for RIP version 2 packets sent and received by this interface. Use <code>auth-string</code> when you only want to configure one key. The key can be up to 35 characters long. | Null |
| receive-version { 1 2 } | RIP routing messages are UDP packets that use port 520. Choose one of: 1 — configure RIP to listen for RIP version 1 messages on an interface. 2 — configure RIP to listen for RIP version 2 messages on an interface. 1 2 — configure RIP to listen for both RIP version 1 and RIP version 2 messages on an interface. | No default. |
| send-version { 1 2 } | RIP routing messages are UDP packets that use port 520. Choose one of: 1 — configure RIP to send for RIP version 1 messages on an interface. 2 — configure RIP to send for RIP version 2 messages on an interface. 1 2 — configure RIP to send for both RIP version 1 and RIP version 2 messages on an interface. | No default. |

| Variable | Description | Default |
|---|---|----------|
| send-version2-broadcast {enable disable} | Enable or disable sending broadcast updates from an interface configured for RIP version 2. RIP version 2 normally multicasts updates. RIP version 1 can only receive broadcast updates. | disable |
| split-horizon {poisoned regular} | Configure RIP to use either regular or poisoned split horizon on this interface. Choose one of: regular — prevent RIP from sending updates for a route back out on the interface from which it received that route. poisoned — send updates with routes learned on an interface back out the same interface but mark those routes as unreachable. | poisoned |
| split-horizon-status {enable disable} | Enable or disable split horizon for this interface. Split horizon is enabled by default. Disable split horizon only if there is no possibility of creating a counting to infinity loop when network topology changes. | enable |

Example

This example shows how to configure the external interface to send and receive RIP version 2, to use MD5 authentication, and to use a key chain called `test1`.

```

config router rip
  config interface
    edit external
      set receive-version 2
      set send-version 2
      set auth-mode md5
      set auth-keychain test1
    end
  end
end

```

config neighbor

Use this subcommand to enable RIP to send unicast routing updates to the router at the specified address. You can use the `neighbor` subcommand and “[passive-interface <name_str>](#)” on [page 424](#) to allow RIP to send unicast updates to the specified neighbor while blocking broadcast updates on the specified interface. You can configure multiple neighbors.

The `ip` field is required. All other fields are optional.

| Variable | Description | Default |
|--------------------|--|-------------|
| edit <neighbor_id> | Enter an ID number for the RIP neighbor. The number must be an integer. | No default. |
| ip <address_ipv4> | Enter the IPv4 address of the neighboring router to which to send unicast updates. | 0.0.0.0 |

Example

This example shows how to specify that the router at 192.168.21.20 is a neighbor.

```
config router rip
  config neighbor
    edit 1
      set ip 192.168.21.20
    end
  end
```

config network

Use this subcommand to identify the networks for which to send and receive RIP updates. If a network is not specified, interfaces in that network will not be advertised in RIP updates. The `prefix` field is optional.

| Variable | Description | Default |
|---------------------------|---|--------------------|
| edit <network_id> | Enter an entry number for the RIP network. The number must be an integer. | No default. |
| prefix <address_ipv4mask> | Enter the IPv4 address and netmask for the RIP network. | 0.0.0.0 0.0.0.0 |

Example

Use the following command to enable RIP for the interfaces attached to networks specified by the IP address 10.0.0.0 and the netmask 255.255.255.0.

```
config router rip
  config network
    edit 2
      set prefix 10.0.0.0 255.255.255.0
    end
  end
```

config offset-list

Use this subcommand to add the specified offset to the metric (hop count) of a route from the offset list. The `access-list`, `direction`, and `offset` fields are required. All other fields are optional.

| Variable | Description | Default |
|------------------------|--|-------------|
| edit <offset_list_id> | Enter an ID number for the offset list. The number must be an integer. | No default. |
| access-list <name_str> | Enter the name of the access list to use for this offset list. The access list is used to determine which routes to add the metric to. For more information, see “router access-list, access-list6” on page 342 . | Null |
| direction {in out} | Enter <code>in</code> to apply the specified offset to the metrics of routes originating on other routers—incoming routes. Enter <code>out</code> to apply the specified offset to the metrics of routes leaving from the FortiGate unit—outgoing routes. | out |
| interface <name_str> | Enter the name of the interface to match for this offset list. | Null |

| Variable | Description | Default |
|------------------------------|--|---------|
| offset <metric_integer> | Enter the offset number to add to the metric. The metric is the hop count. The <code>metric_integer</code> range is from 1 to 16, with 16 being unreachable. For example if a route has already has a metric of 5, an offset of 10 will increase the metric to 15 for that route. | 0 |
| status {enable disable} | Enable or disable this offset list. | disable |

Example

This example shows how to configure and enable offset list ID number 5. This offset list entry adds a metric of 3 to incoming routes that match the access list named `acc_list1` on the external interface.

```
config router rip
  config offset-list
    edit 5
      set access-list acc_list1
      set direction in
      set interface external
      set offset 3
      set status enable
    end
  end
```

config redistribute

Use this subcommand to advertise routes learned from OSPF, BGP, static routes, or a direct connection to the destination network.

The RIP redistribution table contains four static entries. You cannot add entries to the table. The entries are defined as follows:

- `bgp` — Redistribute routes learned from BGP.
- `connected` — Redistribute routes learned from a direct connection to the destination network.
- `isis` — Redistribute routes learned from ISIS.
- `ospf` — Redistribute routes learned from OSPF.
- `static` — Redistribute the static routes defined in the FortiGate unit routing table.

When you enter the subcommand, end the command with one of the four static entry names (that is, `config redistribute {bgp | connected | isis | ospf | static}`). All fields are optional.

| Variable | Description | Default |
|---------------------------|---|---------|
| metric <metric_integer> | Enter the metric value to be used for the redistributed routes. The <code>metric_integer</code> range is from 0 to 16. | 0 |
| route-map <name_str> | Enter the name of the route map to use for the redistributed routes. For information on how to configure route maps, see “router route-map” on page 438 . | Null. |
| status {enable disable} | Enable or disable advertising non-RIP routes. | disable |

ripng

Use this command to configure the “next generation” Routing Information Protocol (RIPng) on the FortiGate unit. RIPng is a distance-vector routing protocol intended for small, relatively homogeneous, IPv6 networks. RIPng uses hop count as its routing metric. Each network is usually counted as one hop. The network diameter is limited to 15 hops. RIPng is defined in RFC 2080.

Syntax

```
config router ripng
    set default-information-originate {enable | disable}
    set default-metric <metric_integer>
    set garbage-timer <timer_integer>
    set passive-interface <name_str>
    set timeout-timer <timer_integer>
    set update-timer <timer_integer>
    config aggregate-address
        edit <entry-id>
            set prefix6 <aggregate_prefix>
        end
    config distance
        edit <distance_id>
            set access-list6 <name_str>
            set distance <distance_int>
            set prefix6 <address_ipv6mask>
        end
    edit <entry-id>config distribute-list
        edit <distribute_list_id>
            set direction {in | out}
            set interface <name_str>
            set listname <access/prefix-listname_str>
            set status {enable | disable}
        end
    config interface
        edit <interface_name>
            set split-horizon {poisoned | regular}
            set split-horizon-status {enable | disable}
        end
    config neighbor
        edit <neighbor_id>
            set ip <address_ipv4>
        end
    config offset-list
        edit <offset_list_id>
            set access-list <name_str>
            set direction {in | out}
            set interface <name_str>
            set offset <metric_integer>
```



```

        set status {enable | disable}
    end
    config redistribute {connected | static | ospf | bgp}
        set metric <metric_integer>
        set routemap <name_str>
        set status {enable | disable}
    end

```

All fields are optional.

| Variable | Description | Default |
|---|---|-------------|
| default-information-originate {enable disable} | Enter <code>enable</code> to advertise a default static route into RIPng. | disable |
| default-metric <metric_integer> | For non-default routes in the static routing table and directly connected networks the default metric is the metric that the FortiGate unit advertises to adjacent routers. This metric is added to the metrics of learned routes. The default metric can be a number from 1 to 16. | 1 |
| garbage-timer <timer_integer> | The time in seconds that must elapse after the timeout interval for a route expires, before RIPng deletes the route. If RIPng receives an update for the route after the timeout timer expires but before the garbage timer expires then the entry is switched back to reachable. RIP timer defaults are effective in most configurations. All routers and access servers in the network should have the same RIP timer settings. The update timer interval can not be larger than the garbage timer interval. Range 5 to 2 147 483 647 seconds. | 120 |
| passive-interface <name_str> | Block RIPng broadcasts on the specified interface. You can use “ config neighbor ” on page 429 and the passive interface command to allow RIPng to send unicast updates to the specified neighbor while blocking broadcast updates on the specified interface. | No default. |

| Variable | Description | Default |
|----------------------------------|--|---------|
| timeout-timer <timer_integer> | <p>The time interval in seconds after which a route is declared unreachable. The route is removed from the routing table. RIP holds the route until the garbage timer expires and then deletes the route. If RIP receives an update for the route before the timeout timer expires, then the timeout-timer is restarted. If RIP receives an update for the route after the timeout timer expires but before the garbage timer expires then the entry is switched back to reachable. The value of the timeout timer should be at least three times the value of the update timer.</p> <p>RIP timer defaults are effective in most configurations. All routers and access servers in the network should have the same RIP timer settings.</p> <p>The update timer interval can not be larger than the timeout timer interval.</p> <p>Range 5 to 2 147 483 647 seconds.</p> | 180 |
| update-timer <timer_integer> | <p>The time interval in seconds between RIP updates.</p> <p>RIP timer defaults are effective in most configurations. All routers and access servers in the network should have the same RIP timer settings.</p> <p>The update timer interval can not be larger than timeout or garbage timer intervals.</p> <p>Range 5 to 2 147 483 647 seconds.</p> | 30 |

config aggregate-address

Use this subcommand to configure aggregate address prefixes.

| Variable | Description | Default |
|----------------------------|---|---------|
| edit <entry-id> | Enter an entry number for the aggregate address list. | |
| prefix6 <aggregate_prefix> | Enter the prefix for the aggregate address. | ::/0 |

config distance

Use this subcommand to specify an administrative distance. When different routing protocols provide multiple routes to the same destination, the administrative distance sets the priority of those routes. The lowest administrative distance indicates the preferred route. The `distance` field is required. All other fields are optional.

If you specify a prefix, RIP uses the specified distance when the source IP address of a packet matches the prefix.

| Variable | Description | Default |
|-------------------------|--|-------------|
| edit <distance_id> | Enter an ID number for the distance. The number must be an integer. | No default. |
| access-list6 <name_str> | Enter the name of an access list. The distances associated with the routes in the access list will be modified. To create an access list, see “router access-list, access-list6” on page 342 . | Null |

| Variable | Description | Default |
|-------------------------------|--|---------|
| distance <distance_int> | Enter a number from 1 to 255, to set the administrative distance. This field is required. | 0 |
| prefix6 <address_ipv6mask> | Optionally enter a prefix to apply the administrative distance to. | ::/0 |

Example

This example shows how to change the administrative distance to 10 for all IP addresses that match the `internal_example` access-list.

```
config router rip
  config distance
    edit 1
      set distance 10
      set access-list internal_example
    end
  end
```

config distribute-list

Use this subcommand to filter incoming or outgoing updates using an access list or a prefix list. If you do not specify an interface, the filter will be applied to all interfaces. You must configure the access list or prefix list that you want the distribution list to use before you configure the distribution list. For more information on configuring access lists and prefix lists, see [“router access-list, access-list6” on page 342](#) and [“router prefix-list, prefix-list6” on page 421](#).

The `direction` and `listname` fields are required. All other fields are optional.

| Variable | Description | Default |
|---------------------------|---|-------------|
| edit <distribute_list_id> | Enter an entry number for the distribution list. The number must be an integer. | No default. |
| direction {in out} | Set the direction for the filter. Enter <code>in</code> to filter incoming packets. Enter <code>out</code> to filter outgoing packets. | out |
| interface <name_str> | Enter the name of the interface to apply this distribution list to. If you do not specify an interface, this distribution list will be used for all interfaces. | Null |
| listname <listname_str> | Enter the name of the access list or prefix list to use for this distribution list. | Null |
| status {enable disable} | Enable or disable this distribution list. | disable |

config interface

Use this subcommand to configure and enable split horizon. All fields are optional.

A split horizon occurs when a router advertises a route it learns over the same interface it learned it on. In this case the router that gave the learned route to the last router now has two entries to get to another location. However, if the primary route fails that router tries the second route to find itself as part of the route and an infinite loop is created. A poisoned split horizon will still advertise the route on the interface it received it on, but it will mark the route as

unreachable. Any unreachable routes are automatically removed from the routing table. This is also called split horizon with poison reverse.

| Variable | Description | Default |
|--|---|-------------|
| edit <interface_name> | Type the name of the FortiGate unit interface that is linked to the RIP network. The interface might be a virtual IPsec or GRE interface. | No default. |
| split-horizon {poisoned regular} | Configure RIP to use either regular or poisoned split horizon on this interface. Choose one of: regular — prevent RIP from sending updates for a route back out on the interface from which it received that route. poisoned — send updates with routes learned on an interface back out the same interface but mark those routes as unreachable. | poisoned |
| split-horizon-status {enable disable} | Enable or disable split horizon for this interface. Split horizon is enabled by default. Disable split horizon only if there is no possibility of creating a counting to infinity loop when network topology changes. | enable |

config neighbor

Use this subcommand to enable RIPng to send unicast routing updates to the router at the specified address. You can use the `neighbor` subcommand and “[passive-interface <name_str>](#)” [on page 424](#) to allow RIPng to send unicast updates to the specified neighbor while blocking broadcast updates on the specified interface. You can configure multiple neighbors.

All fields are required.

| Variable | Description | Default |
|--------------------|--|-------------|
| edit <neighbor_id> | Enter an entry number for the RIPng neighbor. The number must be an integer. | No default. |
| interface <name> | The interface that connects to the neighbor. | No default. |
| ip6 <address_ipv6> | Enter the IP address of the neighboring router to which to send unicast updates. | :: |

config offset-list

Use this subcommand to add the specified offset to the metric (hop count) of a route from the offset list. The `access-list6`, `direction`, and `offset` fields are required. All other fields are optional.

| Variable | Description | Default |
|-------------------------|--|-------------|
| edit <offset_list_id> | Enter an entry number for the offset list. The number must be an integer. | No default. |
| access-list6 <name_str> | Enter the name of the access list to use for this offset list. The access list is used to determine which routes to add the metric to. | Null |
| direction {in out} | Enter <code>in</code> to apply the offset to the metrics of incoming routes. Enter <code>out</code> to apply the offset to the metrics of outgoing routes. | out |
| interface <name_str> | Enter the name of the interface to match for this offset list. | Null |

| Variable | Description | Default |
|---------------------------|--|---------|
| offset <metric_integer> | Enter the offset number to add to the metric. The metric is the hop count. The <code>metric_integer</code> range is from 1 to 16, with 16 being unreachable. | 0 |
| status {enable disable} | Enable or disable this offset list. | disable |

config redistribute

Use this subcommand to redistribute routes learned from OSPF, BGP, static routes, or a direct connection to the destination network.

The RIPng redistribution table contains four static entries. You cannot add entries to the table. The entries are defined as follows:

- `bgp` — Redistribute routes learned from BGP.
- `connected` — Redistribute routes learned from a direct connection to the destination network.
- `isis` — Redistribute routes learned from ISIS.
- `ospf` — Redistribute routes learned from OSPF.
- `static` — Redistribute the static routes defined in the FortiGate unit routing table.

When you enter the subcommand, end the command with one of the four static entry names (that is, `config redistribute {bgp | connected | isis | ospf | static}`).

All fields are optional.

| Variable | Description | Default |
|---------------------------|--|---------|
| metric <metric_integer> | Enter the metric value to be used for the redistributed routes. The <code>metric_integer</code> range is from 0 to 16. | 0 |
| roumap <name_str> | Enter the name of the route map to use for the redistributed routes. | Null |
| status {enable disable} | Enable or disable redistributing routes. | disable |

route-map

Use this command to add, edit, or delete route maps. To use the command to limit the number of received or advertised BGP and RIP routes and routing updates using route maps, see [“Using route maps with BGP” on page 440](#), and RIP [“config redistribute” on page 409](#).

Route maps provide a way for the FortiGate unit to evaluate optimum routes for forwarding packets or suppressing the routing of packets to particular destinations. Compared to access lists, route maps support enhanced packet-matching criteria. In addition, route maps can be configured to permit or deny the addition of routes to the FortiGate unit routing table and make changes to routing information dynamically as defined through route-map rules.

The FortiGate unit compares the rules in a route map to the attributes of a route. The rules are examined in ascending order until one or more of the rules in the route map are found to match one or more of the route attributes:

- When a single matching `match-*` rule is found, changes to the routing information are made as defined through the rule's `set-ip-nexthop`, `set-metric`, `set-metric-type`, and/or `set-tag` settings.
- If no matching rule is found, no changes are made to the routing information.
- When more than one `match-*` rule is defined, all of the defined `match-*` rules must evaluate to TRUE or the routing information is not changed.
- If no `match-*` rules are defined, the FortiGate unit makes changes to the routing information only when all of the default `match-*` rules happen to match the attributes of the route.

The default rule in the route map (which the FortiGate unit applies last) denies all routes. For a route map to take effect, it must be called by a FortiGate unit routing process.



Any fields and rules that do not appear here can be found in the BGP route-map section. See [“Using route maps with BGP” on page 440](#).

Syntax

```
config router route-map
  edit <route_map_name>
    set comments <string>
    config rule
      edit <route_map_rule_id>
        set action {deny | permit}
        set match-interface <name_str>
        set match-ip-address <access/prefix-listname_str>
        set match-ip-nexthop <access/prefix-listname_str>
        set match-metric <metric_integer>
        set match-route-type {1 | 2}
        set match-tag <tag_integer>
        set set-ip-nexthop <address_ipv4>
        set set-metric <metric_integer>
        set set-metric-type {1 | 2}
        set set-tag <tag_integer>
      end
    end
  end
```

All fields are optional.

| Variable | Description | Default |
|---|--|----------------|
| edit <route_map_name> | Enter a name for the route map. | No default. |
| comments <string> | Enter a description for this route map name. | No default. |
| config rule variables | | |
| edit <route_map_rule_id> | Enter an entry number for the rule. The number must be an integer. | No default. |
| action {deny permit} | Enter <code>permit</code> to permit routes that match this rule. Enter <code>deny</code> to deny routes that match this rule. | permit |
| match-interface <name_str> | Enter the name of the local FortiGate unit interface that will be used to match route interfaces. | Null |
| match-ip-address <access/prefix-listname_str> | Match a route if the destination address is included in the specified access list or prefix list. | Null |
| match-ip6-address <access/prefix-listname_str> | Match a route if the destination IPv6 address is included in the specified access6 list or prefix6 list. | Null |
| match-ip-nexthop <access/prefix-listname_str> | Match a route that has a next-hop router address included in the specified access list or prefix list. | Null |
| match-ip6-nexthop <access/prefix-listname_str> | Match a route that has a next-hop router address included in the specified access6 list or prefix6 list. | Null |
| match-metric <metric_integer> | Match a route with the specified metric. The metric can be a number from 1 to 16. | 0 |
| match-route-type {1 2} | Match a route that has the external type set to 1 or 2. | external-type1 |
| match-tag <tag_integer> | This field is available when <code>set-tag</code> is set. Match a route that has the specified tag. | 0 |
| set-ip-nexthop <address_ipv4> | Set the next-hop router address for a matched route. | 0.0.0.0 |
| set-ip6-nexthop <address_ipv6> | Set the next-hop router IPv6 address for a matched route. | ::0 |
| set-ip6-nexthop-local <address_ipv6> | Set the next-hop router local IPv6 address for a matched route. | ::0 |
| set-metric <metric_integer> | Set a metric value of 1 to 16 for a matched route. | 0 |
| set-metric-type {1 2} | Set the type for a matched route. | external-type1 |
| set-tag <tag_integer> | Set a tag value for a matched route. | 0 |

Example

This example shows how to add a route map list named `rtmp2` with two rules. The first rule denies routes that match the IP addresses in an access list named `acc_list2`. The second rule permits routes that match a metric of 2 and changes the metric to 4.

```
config router route-map
  edit rtmp2
  config rule
    edit 1
      set match-ip-address acc_list2
      set action deny
    next
    edit 2
      set match-metric 2
      set action permit
      set set-metric 4
  end
end
```

Using route maps with BGP

When a connection is established between BGP peers, the two peers exchange all of their BGP route entries. Afterward, they exchange updates that only include changes to the existing routing information. Several BGP entries may be present in a route-map table. You can limit the number of received or advertised BGP route and routing updates using route maps. Use the `config router route-map` command to create, edit, or delete a route map.



When you specify a route map for the `dampening-route-map` value through the `config router bgp` command (see [“dampening-route-map <routermap-name_str>” on page 352](#)), the FortiGate unit ignores global dampening settings. You cannot set global dampening settings for the FortiGate unit and then override those values through a route map.

Syntax

```
config router route-map
  edit <route_map_name>
    set comments <string>
  config rule
    edit <route_map_rule_id>
      set match-as-path <aspath-list-name_str>
      set match-community <community-list-name_str>
      set match-community-exact {enable | disable}
      set match-origin {egp | igp | incomplete | none}
      set set-aggregator-as <id_integer>
      set set-aggregator-ip <address_ipv4>
      set set-aspath <id_integer> <id_integer> <id_integer> ...
      set set-atomic-aggregate {enable | disable}
      set set-community-delete <community-list-name_str>
      set set-community <criteria>
      set set-community-additive {enable | disable}
```



```

set set-dampening-reachability-half-life <minutes>
set set-dampening-reuse <reuse_integer>
set set-dampening-suppress <suppress_integer>
set set-dampening-max-suppress <minutes>
set set-dampening-unreachability-half-life <minutes>
set set-extcommunity-rt <AA:NN> <AA:NN> <AA:NN> ...
set set-extcommunity-soo <AA:NN> <AA:NN> <AA:NN> ...
set set-local-preference <preference_integer>
set set-originator-id <address_ipv4>
set set-origin {egp | igp | incomplete | none}
set set-weight <weight_integer>

end

```

All fields are optional.

| Variable | Description | Default |
|---|---|-------------|
| edit <route_map_name> | Enter a name for the route map. | No default. |
| comments <string> | Enter a description for this route map name. | No default. |
| config rule variables | | |
| edit <route_map_rule_id> | Enter an entry number for the rule. The number must be an integer. | No default. |
| match-as-path <aspath-list-name_str> | Enter the AS-path list name that will be used to match BGP route prefixes. You must create the AS-path list before it can be selected here. See “router aspath-list” on page 344 . | Null |
| match-community <community-list-name_str> | Enter the community list name that will be used to match BGP routes according to their COMMUNITY attributes. You must create the community list before it can be selected here. See “router community-list” on page 367 . | Null |
| match-community-exact {enable disable} | This field is only available when match-community is set. Enable or disable an exact match of the BGP route community specified by the match-community field. | disable |
| match-origin {egp igp incomplete none} | Enter a value to compare to the ORIGIN attribute of a routing update: egp — set the value to the NLRI learned from the Exterior Gateway Protocol (EGP). The FortiGate unit has the second-highest preference for routes of this type. igp — set the value to the NLRI learned from a protocol internal to the originating AS. The FortiGate unit has the highest preference for routes learned through Internal Gateway Protocol (IGP). incomplete — match routes that were learned some other way (for example, through redistribution). none — disable the matching of BGP routes based on the origin of the route. | none |

| Variable | Description | Default |
|---|--|-------------|
| set-aggregator-as <id_integer> | Set the originating AS of an aggregated route. The value specifies at which AS the aggregate route originated. The range is from 1 to 65 535. The <code>set-aggregator-ip</code> value must also be set to further identify the originating AS. | unset |
| set-aggregator-ip <address_ipv4> | This field is available when <code>set-aggregator-as</code> is set. Set the IP address of the BGP router that originated the aggregate route. The value should be identical to the FortiGate unit <code>router-id</code> value (see “router-id <address_ipv4>” on page 354). | 0.0.0.0 |
| set-aspath <id_integer> <id_integer> <id_integer> ... | Modify the FortiGate unit AS_PATH attribute and add to it the AS numbers of the AS path belonging to a BGP route. The resulting path describes the autonomous systems along the route to the destination specified by the NLRI. The range is from 1 to 65 535. The <code>set-aspath</code> value is added to the beginning of the AS_SEQUENCE segment of the AS_PATH attribute of incoming routes, or to the end of the AS_SEQUENCE segment of the AS_PATH attribute of outgoing routes. Enclose all AS numbers in quotes if there are multiple occurrences of the same <code>id_integer</code> . Otherwise the AS path may be incomplete. | No default. |
| set-atomic-aggregate { enable disable } | Enable or disable a warning to upstream routers through the ATOMIC_AGGREGATE attribute that address aggregation has occurred on an aggregate route. This value does not have to be specified when an <code>as-set</code> value is specified in the aggregate-address table (see “config aggregate-address, config aggregate-address6” on page 355). | disable |
| set-community-delete <community-list-name_str> | Remove the COMMUNITY attributes from the BGP routes identified in the specified community list. You must create the community list first before it can be selected here (see “router community-list” on page 367). | Null |

| Variable | Description | Default |
|--|---|-------------|
| set-community <criteria> | <p>Set the COMMUNITY attribute of a BGP route.</p> <ul style="list-style-type: none"> Use decimal notation to set a specific COMMUNITY attribute for the route. The value has the syntax AA:NN, where AA represents an AS, and NN is the community identifier. Delimit complex expressions with double-quotation marks (for example, "123:234 345:456"). To make the route part of the Internet community, select <code>internet</code>. To make the route part of the LOCAL_AS community, select <code>local-AS</code>. To make the route part of the NO_ADVERTISE community, select <code>no-advertise</code>. To make the route part of the NO_EXPORT community, select <code>no-export</code>. | No default. |
| set-community-additive {enable disable} | <p>This field is available when <code>set-community</code> is set.</p> <p>Enable or disable the appending of the <code>set-community</code> value to a BGP route.</p> | disable |
| set-dampening-reachability-half-life <minutes> | Set the dampening reachability half-life of a BGP route (in minutes). The range is from 1 to 45. | 0 |
| set-dampening-reuse <reuse_integer> | Set the value at which a dampened BGP route will be reused. The range is from 1 to 20 000. If you set <code>set-dampening-reuse</code> , you must also set <code>set-dampening-suppress</code> and <code>set-dampening-max-suppress</code> . | 0 |
| set-dampening-suppress <suppress_integer> | Set the limit at which a BGP route may be suppressed. The range is from 1 to 20 000. See also " dampening-suppress <limit_integer> " on page 352. | 0 |
| set-dampening-max-suppress <minutes> | Set maximum time (in minutes) that a BGP route can be suppressed. The range is from 1 to 255. See also " dampening-max-suppress-time <minutes_integer> " on page 352. | 0 |
| set-dampening-unreachability-half-life <minutes> | Set the unreachability half-life of a BGP route (in minutes). The range is from 1 to 45. See also " dampening-unreachability-half-life <minutes_integer> " on page 353. | 0 |
| set-extcommunity-rt <AA:NN> <AA:NN> <AA:NN> ... | Set the target extended community (in decimal notation) of a BGP route. The COMMUNITY attribute value has the syntax AA:NN, where AA represents an AS, and NN is the community identifier. | No default. |
| set-extcommunity-soo <AA:NN> <AA:NN> <AA:NN> ... | Set the site-of-origin extended community (in decimal notation) of a BGP route. The COMMUNITY attribute value has the syntax AA:NN, where AA represents an AS, and NN is the community identifier. | No default. |
| set-local-preference <preference_integer> | Set the LOCAL_PREF value of an IBGP route. The value is advertised to IBGP peers. The range is from 0 to 4 294 967 295. A higher number signifies a preferred route among multiple routes to the same destination. | 0 |

| Variable | Description | Default |
|---|---|---------|
| set-originator-id <address_ipv4> | Set the ORIGINATOR_ID attribute, which is equivalent to the <code>router-id</code> of the originator of the route in the local AS. Route reflectors use this value to prevent routing loops. | 0.0.0.0 |
| set-origin {egp igp incomplete none} | Set the ORIGIN attribute of a local BGP route. Choose one of: egp — set the value to the NLRI learned from the Exterior Gateway Protocol (EGP). igp — set the value to the NLRI learned from a protocol internal to the originating AS. incomplete — if not egp or igp . none — disable the ORIGIN attribute. | none |
| set-weight <weight_integer> | Set the weight of a BGP route. A route's weight has the most influence when two identical BGP routes are compared. A higher number signifies a greater preference. The range is from 0 to 2 147 483 647. | 0 |

setting

Use this command to define a prefix list as a filter to show routes.

Command

```
config router setting
  set hostname <name_str>
  set show-filter <prefix_list>
end
```

| Variable | Description | Default |
|---------------------------|--|---------|
| hostname <name_str> | Enter the hostname for this virtual domain router. (1-14 characters) | |
| show-filter <prefix_list> | Select the prefix-list to use as a filter for showing routes. | |

static

Use this command to add, edit, or delete static routes for IPv4 traffic. For IPv6 traffic, use the `static6` command at [“router static6” on page 448](#).

You add static routes to manually control traffic exiting the FortiGate unit. You configure routes by specifying destination IP addresses and network masks and adding gateways for these destination addresses. Gateways are the next-hop routers to which traffic that matches the destination addresses in the route are forwarded.

You can adjust the administrative distance of a route to indicate preference when more than one route to the same destination is available. The lower the administrative distance, the greater the preferability of the route. If the routing table contains several entries that point to the same destination (the entries may have different gateways or interface associations), the FortiGate unit compares the administrative distances of those entries, selects the entries having the lowest distances, and installs them as routes in the FortiGate unit forwarding table. Any ties are resolved by comparing the routes’ priority, with lowest priority being preferred. As a result, the FortiGate unit forwarding table only contains routes having the lowest distances to every possible destination. If both administrative distance and priority are tied for two or more routes, an equal cost multi-path (ECMP) situation occurs. ECMP is available to static and OSPF routing. By default in ECMP, a source IP address hash will be used to determine the selected route. This hash value is based on the pre-NATed source IP address. This method results in all traffic originating from the same source IP address always using the same path. This is the Source based ECMP option, with Weighted, and Spill-over being the other two optional methods. The option is determined by the CLI command `set v4-ecmp-mode` in `config system` setting. Source Based is the default method. Weighted ECMP uses the weight field to direct more traffic to routes with larger weights. In spill-over or usage-based ECMP, the FortiGate unit distributes sessions among ECMP routes based on how busy the FortiGate interfaces added to the routes are. For more information on ECMP, see [“system settings” on page 670](#).

Syntax

```
config router static
  edit <sequence_number>
    set blackhole {enable | disable}
    set device <interface_name>
    set distance <distance>
    set dst <destination-address_ipv4mask>
    set dynamic-gateway {enable | disable}
    set gateway <gateway-address_ipv4>
    set priority <integer>
    set weight <integer>
  end
```

The `dst` and `gateway` fields are required when `blackhole` is disabled. When `blackhole` is enabled, the `dst` field is required. All other fields are optional.

| Variable | Description | Default |
|---------------------------------|--|-------------|
| edit <sequence_number> | Enter a sequence number for the static route. The sequence number may influence routing priority in the FortiGate unit forwarding table. | No default. |
| blackhole {enable disable} | Enable or disable dropping all packets that match this route. This route is advertised to neighbors through dynamic routing protocols as any other static route. | disable |

| Variable | Description | Default |
|---------------------------------------|--|--------------------|
| device <interface_name> | This field is available when <code>blackhole</code> is set to <code>disable</code> . Enter the name of the FortiGate unit interface through which to route traffic. Use '?' to see a list of interfaces. | Null |
| distance <distance> | Enter the administrative distance for the route. The distance value may influence route preference in the FortiGate unit routing table. The range is an integer from 1-255. See also config system interface "distance <distance_integer>" on page 259 . | 10 |
| dst <destination-address_ipv4mask> | Enter the destination IPv4 address and network mask for this route. You can enter <code>0.0.0.0 0.0.0.0</code> to create a new static default route. | 0.0.0.0 0.0.0.0 |
| dynamic-gateway {enable disable} | When enabled, dynamic-gateway hides the gateway variable for a dynamic interface, such as a DHCP or PPPoE interface. When the interface connects or disconnects, the corresponding routing entries are updated to reflect the change. | disable |
| gateway <gateway-address_ipv4> | This field is available when <code>blackhole</code> is set to <code>disable</code> . Enter the IPv4 address of the next-hop router to which traffic is forwarded. | 0.0.0.0 |
| priority <integer> | The administrative priority value is used to resolve ties in route selection. In the case where both routes have the same priority, such as equal cost multi-path (ECMP), the IP source hash (based on the pre-NATed IP address) for the routes will be used to determine which route is selected. The priority range is an integer from 0 to 4294967295. Lower priority routes are preferred routes. This field is only accessible through the CLI. | 0 |
| weight <integer> | Add weights to ECMP static routes if the ECMP route failover and load balance method is set to <code>weighted</code> . Enter weights for ECMP routes. More traffic is directed to routes with higher weights. This option is available when the <code>v4-ecmp-mode</code> field of the <code>config system settings</code> command is set to <code>weight-based</code> . For more information, see "system settings" on page 670 . | 0 |

static6

Use this command to add, edit, or delete static routes for IPv6 traffic. For IPv4 static routes, see [“router static” on page 446](#).

You add static routes to specify the destination of traffic exiting the FortiGate unit. You configure routes by adding destination IP addresses and network masks and adding gateways for these destination addresses. The gateways are the next-hop routers to which traffic that matches the destination addresses in the route are forwarded.



You can configure static routes for IPv6 traffic on FortiGate units that run in NAT/Route mode.

Syntax

```
config router static6
  edit <sequence_number>
    set device <interface_name>
    set distance <distance>
    set dst <destination-address_ipv6mask>
    set gateway <gateway-address_ipv6>
    set priority <integer>
  end
```

The device, dst, and gateway fields are all required.

| Variable | Description | Default |
|---------------------------------------|--|-------------|
| edit <sequence_number> | Enter a sequence number for the static route. | No default. |
| device <interface_name> | The name of the FortiGate unit interface through which to route traffic. | Null |
| distance <distance> | Enter the administrative distance for the route. The distance value may influence route preference in the FortiGate unit routing table. The range is an integer from 1-255. See also config system interface “distance <distance_integer>” on page 259 . | 10 |
| dst <destination-address_ipv6mask> | The destination IPv6 address and netmask for this route. You can enter ::/0 to create a new static default route for IPv6 traffic. | ::/0 |
| gateway <gateway-address_ipv6> | The IPv6 address of the next-hop router to which traffic is forwarded. | :: |
| priority <integer> | The administrative priority value is used to resolve ties in route selection. The priority range is an integer from 0 to 4294967295. Lower priority routes are preferred routes. This field is only accessible through the CLI. | 0 |

spamfilter

Use email filter commands to create a banned word list, configure filters based on email addresses, ip addresses, and MIME headers, and to configure the FortiGuard-Antispam service.

This chapter contains the following sections:

[bwl](#)

[bword](#)

[dnsbl](#)

[fortishield](#)

[iptrust](#)

[mheader](#)

[options](#)

[profile](#)

bwl

Use this command to filter email based on the sender's email address or address pattern.

The FortiGate email filters are applied in the following order:

For SMTP

1. IP address BWL check - Last hop IP
2. DNSBL & ORDBL check, IP address FortiGuard check, HELO DNS lookup
3. E-mail address BWL check
4. MIME headers check
5. IP address BWL check (for IPs extracted from "Received" headers)
6. Return e-mail DNS check, FortiGuard Antispam check (for IPs extracted from "Received" headers, and URLs in email content)
7. Banned word check

For POP3 and IMAP

1. E-mail address BWL check
2. MIME headers check, IP BWL check
3. Return e-mail DNS check, FortiGuard Antispam check, DNSBL & ORDBL check
4. Banned word check

For SMTP, POP3, and IMAP using the email address

The FortiGate unit compares the email address or domain of the sender to the list in sequence. If a match is found, the corresponding action is taken. If no match is found, the email is passed on to the next email filter.

The FortiGate unit can filter email from specific senders or all email from a domain (such as example.net). Each email address can be marked as clear or spam.

Use Perl regular expressions or wildcards to add email address patterns to the list.

Use this command to filter email based on the IP or subnet address.

The FortiGate email filters are generally applied in the following order:

For SMTP, POP3, and IMAP using the IP address

The FortiGate unit compares the IP address of the sender to the list in sequence. If a match is found, the corresponding action is taken. If no match is found, the email is passed on to the next email filter.

Enter an IP address and mask in one of two formats:

- x.x.x.x/x.x.x.x, for example 192.168.10.23/255.255.255.0
- x.x.x.x/x, for example 192.168.10.23/24

Configure the FortiGate unit to filter email from specific IP addresses. Mark each IP address as clear, spam, or reject. Filter single IP addresses, or a range of addresses at the network level by configuring an address and mask.

Syntax

```

config spamfilter bwl
  edit <list_int>
    set name <list_str>
    set comment <comment_str>
  config entries
    edit <entry_id>
      set type email
      set action {clear | spam}
      set email-pattern <email_str>
      set pattern-type {regexp | wildcard}
      set status {enable | disable}
    end
    edit <entry_id>
      set type ip
      set action {clear | reject | spam}
      set addr-type {ipv4 | ipv6}
      set ip4-subnet {<address_ipv4mask>}
      set ip6-subnet {<address_ipv6mask>}
      set status {enable | disable}
    end
  end
end

```

| Variable | Description | Default |
|------------------------------------|--|------------|
| <list_int> | A unique number to identify the email black/white list. | |
| <list_str> | The name of the email black/white list. | |
| <comment_str> | The comment attached to the email black/white list. | |
| <entry_id> | A unique number to identify the entry. | |
| type {email ip} | Select whether pattern is by email address or IP address. | ip |
| action {clear spam} | If type is email: Enter <code>clear</code> to exempt the email from the rest of the spam filters. Enter <code>spam</code> to apply the spam action configured in the profile. | spam |
| action {clear reject spam} | If type is ip: Enter <code>clear</code> to exempt the email from the rest of the email filters. Enter <code>reject</code> to drop any current or incoming sessions. Enter <code>spam</code> to apply the spam action. | spam |
| addr-type {ipv4 ipv6} | Select whether IPv4 or IPv6 addresses will be used. Available if type is ip. | ipv4 |
| email-pattern <email_str> | Enter the email address pattern using wildcards or Perl regular expressions. Available if type is email. | |
| ip4-subnet {<address_ipv4mask>} | The trusted IPv4 IP address and subnet mask in the format 192.168.10.23 255.255.255.0 or 192.168.10.23/24. Available if type is ip. | No default |
| ip6-subnet {<address_ipv6mask>} | The trusted IPv6 IP address. This is available when type is ip and addr-type is ipv6. | No default |

| Variable | Description | Default |
|------------------------------------|--|----------|
| pattern-type {regex wildcard} | Enter the pattern-type for the email address. Choose from wildcards or Perl regular expressions. Available if type is email. | wildcard |
| status {enable disable} | Enable or disable scanning for each email address. | enable |

bword

Use this command to add or edit and configure options for the email filter banned word list.

The FortiGate email filters are applied in the following order:

For SMTP

1. IP address BWL check - Last hop IP
2. DNSBL & ORDBL check, IP address FortiGuard check, HELO DNS lookup
3. E-mail address BWL check
4. MIME headers check
5. IP address BWL check (for IPs extracted from “Received” headers)
6. Return e-mail DNS check, FortiGuard Antispam check (for IPs extracted from “Received” headers, and URLs in email content)
7. Banned word check

For POP3 and IMAP

1. E-mail address BWL check
2. MIME headers check, IP BWL check
3. Return e-mail DNS check, FortiGuard Antispam check, DNSBL & ORDBL check
4. Banned word check

For SMTP, POP3, and IMAP

Control spam by blocking email messages containing specific words or patterns. If enabled, the FortiGate unit searches for words or patterns in email messages. If matches are found, values assigned to the words are totalled. If a user-defined threshold value is exceeded, the message is marked as spam. If no match is found, the email message is passed along to the next filter.

Use Perl regular expressions or wildcards to add banned word patterns to the list. Add one or more banned words to sort email containing those words in the email subject, body, or both. Words can be marked as spam or clear. Banned words can be one word or a phrase up to 127 characters long.

If a single word is entered, the FortiGate unit blocks all email that contain that word. If a phrase is entered, the FortiGate unit blocks all email containing the exact phrase. To block any word in a phrase, use Perl regular expressions.



Perl regular expression patterns are case sensitive for email filter banned words. To make a word or phrase case insensitive, use the regular expression `/i`. For example, `/bad language/i` blocks all instances of `bad language` regardless of case. Wildcard patterns are not case sensitive.

Syntax

```

config spamfilter bword
  edit <list_int>
    set name <list_str>
    set comment <comment_str>
  config entries
    edit <banned_word_int>
      set action {clear | spam}
      set language {french | japanese | korean | simch | spanish
        | thai | trach | western}
      set pattern <banned_word_str>
      set pattern-type {regex | wildcard}
      set score <int>
      set status {enable | disable}
      set where {all | body | subject}
    end
  end

```

| Variable | Description | Default |
|--|--|-------------|
| <list_int> | A unique number to identify the banned word list. | |
| <list_str> | The name of the banned word list. | |
| <comment_str> | The comment attached to the banned word list. | |
| <banned_word_int> | A unique number to identify the banned word or pattern. | |
| action {clear spam} | Enter <code>clear</code> to allow the email. Enter <code>spam</code> to apply the spam action. | spam |
| language {french japanese korean simch spanish thai trach western} | Enter the language character set used for the banned word or phrase. Choose from French, Japanese, Korean, Simplified Chinese, Thai, Traditional Chinese, or Western. | western |
| pattern <banned_word_str> | Enter the banned word or phrase pattern using regular expressions or wildcards. | No default. |
| pattern-type {regex wildcard} | Enter the pattern type for the banned word (pattern). Choose from regular expressions or wildcard. | wildcard |
| score <int> | A numerical weighting applied to the banned word. The score values of all the matching words appearing in an email message are added, and if the total is greater than the <code>spamwordthreshold</code> value, the message is processed according to the spam action setting. The score for a banned word is counted once even if the word appears multiple times in an email message. | 10 |
| status {enable disable} | Enable or disable scanning email for each banned word. | enable |
| where {all body subject} | Enter where in the email to search for the banned word or phrase. | all |

dnsbl

Use this command to configure email filtering using DNS-based Blackhole List (DNSBL) or Open Relay Database List (ORDBL) servers. DSNBL and ORDBL settings are configured with this command but DSNBL and ORDBL filtering is enabled within each profile.

The FortiGate email filters are generally applied in the following order:

For SMTP

1. IP address BWL check - Last hop IP
2. DNSBL & ORDBL check, IP address FortiGuard check, HELO DNS lookup
3. E-mail address BWL check
4. MIME headers check
5. IP address BWL check (for IPs extracted from “Received” headers)
6. Return e-mail DNS check, FortiGuard Antispam check (for IPs extracted from “Received” headers, and URLs in email content)
7. Banned word check

For POP3 and IMAP

1. E-mail address BWL check
2. MIME headers check, IP BWL check
3. Return e-mail DNS check, FortiGuard Antispam check, DNSBL & ORDBL check
4. Banned word check

For SMTP, POP3, and IMAP

The FortiGate unit compares the IP address or domain name of the sender to any database lists configured in sequence. If a match is found, the corresponding action is taken. If no match is found, the email is passed on to the next email filter.

Some spammers use unsecured third party SMTP servers to send unsolicited bulk email. Using DNSBLs and ORDBLs is an effective way to tag or reject spam as it enters the network. These lists act as domain name servers that match the domain of incoming email to a list of IP addresses known to send spam or allow spam to pass through.

There are several free and subscription servers available that provide reliable access to continually updated DNSBLs and ORDBLs. Please check with the service being used to confirm the correct domain name for connecting to the server.



Because the FortiGate unit uses the server domain name to connect to the DNSBL or ORDBL server, it must be able to look up this name on the DNS server. For information on configuring DNS, see [“system dns” on page 508](#).

Syntax

```

config spamfilter dnsbl
    edit <list_int>
        set name <list_str>
        set comment <comment_str>
    config entries
        edit <server_int>
            set action {reject | spam}
            set server <fqdn>
            set status {enable | disable}
        end
    end
end

```

| Variable | Description | Default |
|---------------------------|--|-------------|
| <list_int> | A unique number to identify the DNSBL list. | |
| <list_str> | The name of the DNSBL header list. | |
| <comment_str> | The comment attached to the DNSBL header list. | |
| <server_int> | A unique number to identify the DNSBL server. | |
| action {reject spam} | Enter <code>reject</code> to stop any further processing of the current session and to drop an incoming connection at once. Enter <code>spam</code> to identify email as spam. | spam |
| server <fqdn> | Enter the domain name of a DNSBL server or an ORDBL server. | No default. |
| status {enable disable} | Enable or disable querying the server named in the server string. | enable |

fortishield

Use this command to configure the settings for the FortiGuard-Antispam Service.

The FortiGate email filters are applied in the following order:

For SMTP

1. IP address BWL check - Last hop IP
2. DNSBL & ORDBL check, IP address FortiGuard check, HELO DNS lookup
3. E-mail address BWL check
4. MIME headers check
5. IP address BWL check (for IPs extracted from “Received” headers)
6. Return e-mail DNS check, FortiGuard Antispam check (for IPs extracted from “Received” headers, and URLs in email content)
7. Banned word check

For POP3 and IMAP

1. E-mail address BWL check
2. MIME headers check, IP BWL check
3. Return e-mail DNS check, FortiGuard Antispam check, DNSBL & ORDBL check
4. Banned word check

For SMTP, POP3, and IMAP

FortiGuard-Antispam Service is an antispam system from Fortinet that includes an IP address black list, a URL black list, and email filtering tools. The IP address black list contains IP addresses of email servers known to be used to generate Spam. The URL black list contains found in Spam email.

FortiGuard-Antispam Service compiles the IP address and URL list from email captured by spam probes located around the world. Spam probes are email addresses purposely configured to attract spam and identify known spam sources to create the antispam IP address and URL list. FortiGuard-Antispam Service combines IP address and URL checks with other email filter techniques in a two-pass process.

On the first pass, if `spamfsip` is selected in the profile, FortiGuard-Antispam Service extracts the SMTP mail server source address and sends the IP address to a FortiGuard-Antispam Service server to see if this IP address matches the list of known spammers. If `spamfsurl` is selected in the profile, FortiGuard-Antispam Service checks the body of email messages to extract any URL links. These URL links will be sent to a FortiGuard-Antispam Service server to see if any of them is listed. Typically spam messages contain URL links to advertisements (also called spamvertizing).

If an IP address or URL match is found, FortiGuard-Antispam Service terminates the session. If FortiGuard-Antispam Service does not find a match, the mail server sends the email to the recipient.

As each email is received, FortiGuard-Antispam Service performs the second antispam pass by checking the header, subject, and body of the email for common spam content. If FortiGuard-Antispam Service finds spam content, the email is tagged or dropped.

Syntax

```
config spamfilter fortishield
    set spam-submit-force {enable | disable}
    set spam-submit-srv <url_str>
    set spam-submit-txt2htm {enable | disable}
end
```

| Variable | Description | Default |
|---|--|-------------------|
| spam-submit-force {enable disable} | Enable or disable force insertion of a new mime entity for the submission text. | enable |
| spam-submit-srv <url_str> | The host name of the FortiGuard-Antispam Service server. The FortiGate unit comes preconfigured with the host name. Use this command only to change the host name. | www.nospammer.net |
| spam-submit-txt2htm {enable disable} | Enable or disable converting text email to HTML. | enable |

iptrust

Use this command to add an entry to a list of trusted IP addresses.

If the FortiGate unit sits behind a company's Mail Transfer Units, it may be unnecessary to check email IP addresses because they are internal and trusted. The only IP addresses that need to be checked are those from outside of the company. In some cases, external IP addresses may be added to the list if it is known that they are not sources of spam.

Syntax

```
config spamfilter iptrust
  edit <list_int>
    set name <list_str>
    set comment <comment_str>
  config entries
    edit <address_int>
      set addr-type {ipv4 | ipv6}
      set ip4-subnet {<address_ipv4mask>}
      set ip6-subnet {<address_ipv6mask>}
      set status {enable | disable}
    end
  end
```

| Variable | Description | Default |
|------------------------------------|--|------------|
| addr-type {ipv4 ipv6} | Select whether IPv4 or IPv6 addresses will be used. | ipv4 |
| <list_int> | A unique number to identify the IP trust list. | |
| <list_str> | The name of the IP trust list. | |
| <comment_str> | The comment attached to the IP trust list. | |
| <address_int> | A unique number to identify the address. | |
| ip4-subnet {<address_ipv4mask>} | The trusted IPv4 IP address and subnet mask in the format 192.168.10.23 255.255.255.0 or 192.168.10.23/24. | No default |
| ip6-subnet {<address_ipv6mask>} | The trusted IPv6 IP address. This is available when addr-type is ipv6. | No default |
| status {enable disable} | Enable or disable the IP address. | enable |

mheader

Use this command to configure email filtering based on the MIME header. MIME header settings are configured with this command but MIME header filtering is enabled within each profile.

The FortiGate email filters are applied in the following order:

For SMTP

1. IP address BWL check - Last hop IP
2. DNSBL & ORDBL check, IP address FortiGuard check, HELO DNS lookup
3. E-mail address BWL check
4. MIME headers check
5. IP address BWL check (for IPs extracted from “Received” headers)
6. Return e-mail DNS check, FortiGuard Antispam check (for IPs extracted from “Received” headers, and URLs in email content)
7. Banned word check

For POP3 and IMAP

1. E-mail address BWL check
2. MIME headers check, IP BWL check
3. Return e-mail DNS check, FortiGuard Antispam check, DNSBL & ORDBL check
4. Banned word check

For SMTP, POP3, and IMAP

The FortiGate unit compares the MIME header key-value pair of incoming email to the list pair in sequence. If a match is found, the corresponding action is taken. If no match is found, the email is passed on to the next email filter.

MIME (Multipurpose Internet Mail Extensions) headers are added to email to describe content type and content encoding, such as the type of text in the email body or the program that generated the email. Some examples of MIME headers include:

- X-mailer: outgluck
- X-Distribution: bulk
- Content_Type: text/html
- Content_Type: image/jpg

The first part of the MIME header is called the header key, or just header. The second part is called the value. Spammers often insert comments into header values or leave them blank. These malformed headers can fool some spam and virus filters.

Use the MIME headers list to mark email from certain bulk mail programs or with certain types of content that are common in spam messages. Mark the email as spam or clear for each header configured.

Use Perl regular expressions or wildcards to add MIME header patterns to the list. MIME header entries are case sensitive.

Syntax

```

config spamfilter mheader
  edit <list_int>
    set name <list_str>
    set comment <comment_str>
  config entries
    edit <mime_int>
      set action {clear | spam}
      set fieldbody <mime_str>
      set fieldname <mime_str>
      set pattern-type {regex | wildcard}
      set status {enable | disable}
    end
  end
end

```

| Variable | Description | Default |
|---------------------------------|---|-------------|
| <list_int> | A unique number to identify the MIME header list. | |
| <list_str> | The name of the MIME header list. | |
| <comment_str> | The comment attached to the MIME header list. | |
| <mime_int> | A unique number to identify the MIME header. | |
| action {clear spam} | Enter <code>clear</code> to exempt the email from the rest of the email filters. Enter <code>spam</code> to apply the spam action. | spam |
| fieldbody <mime_str> | Enter the MIME header (key, header field body) using wildcards or Perl regular expressions. | No default. |
| fieldname <mime_str> | Enter the MIME header value (header field name) using wildcards or Perl regular expressions. Do not include a trailing colon. | No default. |
| pattern-type {regex wildcard} | Enter the pattern-type for the MIME header. Choose from wildcards or Perl regular expressions. | wildcard |
| status {enable disable} | Enable or disable scanning email headers for the MIME header and header value defined in the <code>fieldbody</code> and <code>fieldname</code> strings. | enable |

options

Use this command to set the spamfilter DNS query timeout.

Syntax

```
config spamfilter options
    set dns-timeout <timeout_int>
end
```

| Variable | Description | Default |
|---------------------------|---|---------|
| dns-timeout <timeout_int> | Set the DNS query timeout in the range 1 to 30 seconds. | 7 |

profile

Use this command to configure UTM email filtering profiles for firewall policies. Email filtering profiles configure how Email filtering and FortiGuard Antispam is applied to sessions accepted by a firewall policy that includes the Email filtering profile.

Syntax

```
config spamfilter profile
edit <name_str>
    set comment <comment_str>
    set flow-based {enable | disable}
    set spam-log {enable | disable}
    set spam-bwl-table <index_int>
    set spam-bword-threshold <value_int>
    set spam-bword-table <index_int>
    set spam-emaddr-table <index_int>
    set spam-filtering {enable | disable}
    set spam-iptrust-table <index_int>
    set spam-mheader-table <index_int>
    set spam-rbl-table <index_int>
    set options {bannedword | spambwl | spamfschksum | spamfsip
                | spamfsphish | spamfssubmit | spamfsurl | spamhdrcheck
                | spamraddrdns | spamrbl}
    config {imap | imaps | mapi | pop3 | pop3s | smtp | smtps}
        set action {discard | pass | tag}
        set log {enable | disable}
        set tag-type {subject | header} [spaminfo]
        set tag-msg <message_str>
        set hdrip {enable | disable}
        set local-override {enable | disable}
    end
    config {gmail | msn-hotmail | yahoo-mail}
        set log {enable | disable}
    end
end
```

| Variable | Description | Default |
|----------------------------------|--|---------|
| <name_str> | Enter the name of the email filtering profile. | |
| comment <comment_str> | Optionally enter a description of up to 63 characters of the email filter profile. | |
| flow-based {enable disable} | Enable or disable flow-based spam filtering. | disable |
| spam-bwl-table <index_int> | Enter the ID number of the email filter IP address black/white list to be used with the profile. | 0 |
| spam-log {enable disable} | Enable or disable logging for email filtering. | disable |

| Variable | Description | Default |
|--|--|--------------|
| spam-bword-threshold <value_int> | If the combined scores of the banned word patterns appearing in an email message exceed the threshold value, the message will be processed according to the Spam Action setting. | 10 |
| spam-bword-table <index_int> | Enter the ID number of the email filter banned word list to be used. | 0 |
| spam-emaddr-table <index_int> | Enter the ID number of the email filter email address list to be used. | 0 |
| spam-filtering { enable disable } | Enable or disable spam filtering. | disable |
| spam-iptrust-table <index_int> | Enter the ID number of the email filter IP trust list to be used with the profile. | 0 |
| spam-mheader-table <index_int> | Enter the ID number of the email filter MIME header list to be used with the profile. | 0 |
| spam-rbl-table <index_int> | Enter the ID number of the email filter DNSBL list to be used with the profile. | 0 |
| options { bannedword spambwl spamfschksum spamfsip spamfspathish spamfssubmit spamfsurl spamhdrcheck spamraddrdns spamrbl } | <p>Select actions, if any, the FortiGate unit will perform with email traffic.</p> <p>bannedword — block email containing content in the banned word list.</p> <p>spambwl — filter email using a black/white list.</p> <p>spamfspathish — detect phishing URLs in email.</p> <p>spamfsip — filter email using the FortiGuard Antispam filtering IP address blacklist.</p> <p>spamfssubmit — add a link to the message body allowing users to report messages incorrectly marked as spam. If an email message is not spam, click the link in the message to report the false positive.</p> <p>spamfsurl — filter email using the FortiGuard Antispam filtering URL blacklist.</p> <p>spamhdrcheck — filter email using the MIME header list.</p> <p>spamaddrdns — filter email using a return email DNS check.</p> <p>spamrbl — filter email using configured DNS-based Blackhole List (DNSBL) and Open Relay Database List (ORDBL) servers.</p> <p>Separate multiple options with a space. To remove an option from the list or add an option to the list, retype the list with the option removed or added.</p> | spamfssubmit |

config {imap | imaps | mapi | pop3 | pop3s | smtp | smtps}

Configure spam filtering options for the IMAP, IMAPS, MAPI, POP3, POP3S, SMTP, and SMTPS email protocols.

| Variable | Description | Default |
|--|--|---------------------|
| action {discard pass tag} | <p>Select the action that this profile uses for filtered email. Tagging appends custom text to the subject or header of email identified as spam. When <code>scan</code> or streaming mode (also called <code>splice</code>) is selected, the FortiGate unit can only discard spam email. Discard immediately drops the connection. Without streaming mode or scanning enabled, chose to discard, pass, or tag spam.</p> <p><code>discard</code> — do not pass email identified as spam.</p> <p><code>pass</code> — disable spam filtering.</p> <p><code>tag</code> — tag spam email with text configured using the <code>tagmsg</code> option and the location set using the <code>tag-type</code> option.</p> | discard |
| log {enable disable} | Enable or disable logging. | disable |
| tag-type {subject header} [spaminfo] | <p>Select to affix the tag to either the MIME header or the subject line, and whether or not to append spam information to the spam header, when an email is detected as spam. Also configure <code>tag-msg</code>.</p> <p>If you select to add the tag to the subject line, the FortiGate unit will convert the entire subject line, including tag, to UTF-8 by default. This improves display for some email clients that cannot properly display subject lines that use more than one encoding.</p> | subject spaminfo |
| tag-msg <message_str> | <p>Enter a word or phrase (tag) to affix to email identified as spam.</p> <p>When typing a tag, use the same language as the FortiGate unit's current administrator language setting. Tagging text using other encodings may not be accepted.</p> <p>To correctly enter the tag, your SSH or telnet client must also support your language's encoding. Alternatively, you can use the web-based manager's CLI widget to enter the tag.</p> <p>Tags must not exceed 64 bytes. The number of characters constituting 64 bytes of data varies by text encoding, which may vary by the FortiGate administrator language setting.</p> <p>Tags containing space characters, such as multiple words or phrases, must be surrounded by quote characters (') to be accepted by the CLI.</p> | Spam |
| hdrrip {enable disable} | For <code>smtp</code> and <code>smtps</code> . Select to check header IP addresses for <code>spamfsip</code> , <code>spamrbl</code> , and <code>spamipbwl</code> filters. | disable |
| local-override {enable disable} | For <code>smtp</code> and <code>smtps</code> . Select to override SMTP or SMTPS remote check, which includes IP RBL check, IP FortiGuard antispam check, and HELO DNS check, with the locally defined black/white antispam list. | disable |

config {gmail | msn-hotmail | yahoo-mail}

Configure spam filtering options for GMail, MSN Hotmail, or Yahoo mail.

| Variable | Description | Default |
|------------------------|----------------------------|---------|
| log {enable disable} | Enable or disable logging. | disable |

switch-controller

Use these commands to manage an external FortiSwitch unit. These commands are available on the FortiGate-100D.

This chapter describes the following commands:

[managed-switch](#)

[vlan](#)

managed-switch

Use this command to configure a managed FortiSwitch unit.

Syntax

```
config switch-controller managed-switch
  edit <switch_id>
    set description <text_str>
    set name <name_str>
    set fsw-wan1-admin {enable | discovered | disable}
    set fsw-wan2-admin {enable | discovered | disable}
    set fsw-wan1-peer <port_str>
    set fsw-wan2-peer <port_str>
  config ports
    edit <port-name>
      set vlan <switch-controller_vlan_name>
      set speed <speed_str>
      set status {up | down}
    end
  end
end
```

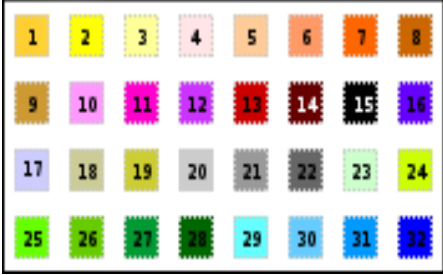
| Variable | Description | Default |
|---|--|-------------|
| <switch_id> | Enter a number to identify this FortiSwitch unit. | No default. |
| description <text_str> | Optionally, enter a description. | No default. |
| name <name_str> | Enter a name to identify this switch | |
| <port-name> | Enter the FortiSwitch port name, such as port1. | |
| fsw-wan1-admin {enable discovered disable} | Set FortiSwitch WAN1 admin status. | |
| fsw-wan2-admin {enable discovered disable} | Set FortiSwitch WAN2 admin status. | |
| fsw-wan1-peer <port_str> | Set FortiSwitch WAN1 peer port. | |
| fsw-wan2-peer <port_str> | Set FortiSwitch WAN2 peer port. | |
| config ports variables | | |
| speed <speed_str> | Set port speed. Enter set speed ? to see a list of valid speed settings. | auto |
| status {up down} | Set port status: up or down. | up |
| vlan <switch-controller_vlan_name> | Enter the name of the VLAN to which this port belongs. | vsw.root |
| Read-only fields | | |
| dot1x-enable | | |
| dot1x-status | | |
| image-download progress | | |

vlan

Use this command to set the switchctl VLAN configuration.

Syntax

```
config switch-controller vlan
edit <switch-VLAN-name>
    set auth {usergroup | radius}
    set color {color_int>}
    set comments <text_str>
    set portal-message-override-group <groupname_str>
    set radius-server <server_str>
    set selected-usergroups <group1> [<group2> ... <groupn>]
    set security {open | captive-portal | 8021x}
    set usergroup <group>
end
```

| Variable | Description | Default |
|--|---|-------------|
| <switch-VLAN-name> | Enter the switch VLAN name. | |
| auth {usergroup radius} | Select authentication by user group or by RADIUS server. available when security is 8021x. | usergroup |
| color {color_int>} | Select the icon color for the web-based manager:  | 1 |
| comments <text_str> | Enter a comment about this VLAN. | |
| portal-message-override-group <groupname_str> | Set the captive portal replacement message override group. This is available when security is captive-portal. | |
| radius-server <server_str> | Enter the IP address or FQDN of the RADIUS server. This is available when security is 8021x and auth is radius. | |
| selected-usergroups <group1> [<group2> ... <groupn>] | Enter the user groups that can authenticate using the captive portal. This is available when security is captive-portal. | No default. |
| security {open captive-portal 8021x} | Select the type of security to apply. open provides no security. | open |
| usergroup <group> | This is available when security is 8021x and auth is usergroup. | No default. |
| Read-only fields | | |
| vlanid <id_int> | Current VLAN ID. Range 1 to 4094. | |
| vdom <vdom_name> | Current VDOM name. | |

system

Use `system` commands to configure options related to the overall operation of the FortiGate unit, including. This chapter contains the following sections:

| | | |
|------------------------|-------------------------------------|--------------------------|
| 3g-modem custom | ha | replacemsg-group |
| accprofile | interface | replacemsg-image |
| admin | ipip-tunnel | replacemsg nac-quar |
| amc | ips-urlfilter-dns | replacemsg nntp |
| arp-table | ipv6-neighbor-cache | replacemsg spam |
| auto-install | ipv6-tunnel | replacemsg sslvpn |
| autoupdate push-update | mac-address-table | replacemsg traffic-quota |
| autoupdate schedule | modem | replacemsg utm |
| autoupdate tunneling | monitors | replacemsg webproxy |
| aux | network-visibility | resource-limits |
| bug-report | np6 | server-probe |
| bypass | npu | session-helper |
| central-management | ntp | session-sync |
| console | object-tag | session-ttl |
| ddns | password-policy | settings |
| dedicated-mgmt | physical-switch | sit-tunnel |
| dhcp reserved-address | port-pair | sflow |
| dhcp server | probe-response | sms-server |
| dhcp6 server | proxy-arp | snmp community |
| dns | pstn | snmp sysinfo |
| dns-database | replacemsg admin | snmp user |
| dns-server | replacemsg alertmail | sp |
| elbc | replacemsg auth | storage |
| email-server | replacemsg device-detection-portal | stp |
| fips-cc | replacemsg ec | switch-interface |
| fortiguard | replacemsg fortiguard-wf | tos-based-priority |
| fortisandbox | replacemsg ftp | vdom-dns |
| geoip-override | replacemsg http | vdom-link |
| gi-gk | replacemsg im | vdom-property |
| global | replacemsg mail | vdom-radius-server |
| gre-tunnel | replacemsg mm1 to replacemsg mm7 | vdom-sflow |

(continued overleaf...)

(continued)

[virtual-switch](#)

[wccp](#)

[zone](#)

3g-modem custom

Use this command to configure the FortiGate unit for an installed 3G wireless PCMCIA modem.

Syntax

```
config system 3g-modem custom
  edit <entry_id>
    set vendor <vendor_str>
    set model <model_str>
    set product-id <pid_hex>
    set vendor-id <vid_hex>
    set class-id <cid_hex>
    set init-str <init_str>
  end
```

| Variable | Description | Default |
|----------------------|---|---------|
| vendor <vendor_str> | Enter the vendor name. | |
| model <model_str> | Enter the modem model name. | |
| product-id <pid_hex> | Enter the USB product ID. Valid range is 0x0000 - 0xFFFF. | |
| vendor-id <vid_hex> | Enter the USB vendor ID. Valid range is 0x0000 - 0xFFFF. | |
| class-id <cid_hex> | Enter the USB interface class. Valid range is 0x00 - 0xFF | |
| init-str <init_str> | Enter the initialization string in hexadecimal format, even length. | |

accprofile

Use this command to add access profiles that control administrator access to FortiGate features. Each FortiGate administrator account must include an access profile. You can create access profiles that deny access, allow read only, or allow both read and write access to FortiGate features.

You cannot delete or modify the super_admin access profile, but you can use the super_admin profile with more than one administrator account.

Syntax

```
config system accprofile
  edit <profile-name>
    set menu-file <filedata>
    set scope {global | vdom}
    set <access-group> <access-level>
  config fwgrp-permission
    set address {none | read | read-write}
    set device {none | read | read-write}
    set others {none | read | read-write}
    set policy {none | read | read-write}
    set profile {none | read | read-write}
    set schedule {none | read | read-write}
    set service {none | read | read-write}
  end
  config loggrp-permission
    set config {none | read | read-write}
    set data-access {none | read | read-write}
  end
  config utmgrp-permission
    set antivirus {none | read | read-write}
    set application-control {none | read | read-write}
    set data-loss-prevention {none | read | read-write}
    set icap {none | read | read-write}
    set ips {none | read | read-write}
    set netscan {none | read | read-write}
    set spamfilter {none | read | read-write}
    set voip {none | read | read-write}
    set webfilter {none | read | read-write}
  end
end
```

| Variable | Description | Default |
|-----------------------|--|-------------|
| edit <profile-name> | Enter a new profile name to create a new profile. Enter an existing profile name to edit that profile. | No default. |
| menu-file <filedata> | Enter the name of the base64-encoded file of data to configure the menu display on the FortiGate unit. For future use. | No default. |
| scope {global vdom} | Enter scope administrator access: global or a single VDOM. | vdom |

| Variable | Description | | Default |
|---|--|--|-------------|
| <access-group> | Enter the feature group for which you are configuring access: | | No default. |
| | admingrp | administrator accounts and access profiles | |
| | authgrp | user authentication, including local users, RADIUS servers, LDAP servers, and user groups | |
| | endpoint-control-grp | endpoint control (Endpoint NAC) configuration | |
| | fwgrp | firewall configuration | |
| | loggrp | log and report configuration including log settings, viewing logs and alert email settings execute batch commands | |
| | mntgrp | maintenance commands: reset to factory defaults, format log disk, reboot, restore and shutdown | |
| | netgrp | interfaces, dhcp servers, zones get system status get system arp table config system arp-table execute dhcp lease-list execute dhcp lease-clear | No default. |
| | routegrp | router configuration | |
| | sysgrp | system configuration except accprofile, admin and autoupdate | |
| | updategrp | FortiGuard antivirus and IPS updates, manual and automatic | |
| | utmgrp | UTM configuration | |
| | vpngrp | VPN configuration | |
| | wanoptgrp | WAN optimization configuration | |
| | wifi | WiFi configuration | |
| <access-level> | Enter the level of administrator access to this feature: | | none |
| | custom | configures custom access for fwgrp, loggrp or utmgrp access selections only | |
| | none | no access | |
| | read | read-only access | |
| | read-write | read and write access | |
| config fwgrp-permission fields. Available if fwgrp is set to custom | | | |
| address { none read read-write } | Enter the level of administrator access to firewall addresses. | | none |
| device { none read read-write } | Enter the level of administrator access to netscan device identification configurations. | | |
| others { none read read-write } | Enter the level of administrator access to virtual IP configurations. | | none |

| Variable | Description | Default |
|---|--|---------|
| policy { none read read-write } | Enter the level of administrator access to firewall policies. | none |
| profile { none read read-write } | Enter the level of administrator access to firewall profiles. | none |
| schedule { none read read-write } | Enter the level of administrator access to firewall schedules. | none |
| service { none read read-write } | Enter the level of administrator access to firewall service definitions. | none |
| config loggrp-permission fields. Available if loggrp is set to custom. | | |
| config { none read read-write } | Enter the level of administrator access to the logging configuration. | none |
| data-access { none read read-write } | Enter the level of administrator access to the log data. | none |
| config utmgrp-permission fields. Available if utmgrp is set to custom. | | |
| antivirus { none read read-write } | Enter the level of administrator access to antivirus configuration data. | none |
| application-control { none read read-write } | Enter the level of administrator access to application control data. | none |
| data-loss-prevention { none read read-write } | Enter the level of administrator access to data loss prevention (DLP) data. | none |
| icap { none read read-write } | Enter the level of administrator access to Internet Content Adaptation Protocol configuration. | none |
| ips { none read read-write } | Enter the level of administrator access to intrusion prevention (IP) data. | none |
| netscan { none read read-write } | Enter the level of administrator access to network scans. | none |
| spamfilter { none read read-write } | Enter the level of administrator access to spamfilter data. | none |
| voip { none read read-write } | Enter the level of administrator access to VOIP data. | none |
| webfilter { none read read-write } | Enter the level of administrator access to web filter data. | none |

admin

Use this command to add, edit, and delete administrator accounts. Administrators can control what data modules appear in the FortiGate unit system dashboard by using the `config system admin` command. Administrators must have read and write privileges to make dashboard web-based manager modifications.

Use the default admin account or an account with system configuration read and write privileges to add new administrator accounts and control their permission levels. Each administrator account except the default admin must include an access profile. You cannot delete the default super admin account or change the access profile (super_admin). In addition, there is also an access profile that allows read-only super admin privileges, super_admin_readonly. The super_admin_readonly profile cannot be deleted or changed, similar to the super_admin profile. This read-only super-admin may be used in a situation where it is necessary to troubleshoot a customer configuration without making changes.

You can authenticate administrators using a password stored on the FortiGate unit or you can perform authentication with RADIUS, LDAP, or TACACS+ servers. When you use RADIUS authentication, you can authenticate specific administrators or you can allow any account on the RADIUS server to access the FortiGate unit as an administrator.



For users with super_admin access profile, you can reset the password in the CLI.

For a user ITAdmin with the access profile super_admin, to set the password to 123456:

```
config system admin
  edit ITAdmin
    set password 123456
  end
```

For a user ITAdmin with the access profile super_admin, to reset the password from 123456 to the default 'empty' or 'null':

```
config system admin
  edit ITAdmin
    unset password 123456
  end
```

If you type 'set password ?' in the CLI, you will have to enter the new password and the old password in order for the change to be effective. In this case, you will NOT be able to reset the password to 'empty' or 'null'.

You can configure an administrator to only be allowed to log in at certain times. The default setting allows administrators to log in any time.

A vdom/access profile override feature supports authentication of administrators via RADIUS. The admin user will have access depending on which vdom they are restricted to and their associated access profile. This feature is only available to wildcard admins. There can only be one vdom-override user per system.

You can define trusted hosts for all of your administrators to increase the security of your network by further restricting administrative access. When you set trusted hosts for all administrators, the FortiGate unit does not respond to administrative access attempts from any other hosts. The trusted hosts you define apply both to the web-based manager and to the CLI when accessed through Telnet or SSH. CLI access through the console connector is not affected.

Syntax

```

config system admin
  edit <name_str>
    set accprofile <profile-name>
    set accprofile-override {enable | disable}
    set allow-remove-admin-session {enable | disable}
    set comments <comments_string>
    set force-password-change {enable | disable}
    set guest-auth {enable | disable}
    set guest-usergroups <groups_list>
    set gui-log-display { | fortianalyzer | fortiguard
      | memory | disk}
    set {ip6-trusthost1 | ip6-trusthost2 | ip6-trusthost3
      | ip6-trusthost4 | ip6-trusthost5 | ip6-trusthost6
      | ip6-trusthost7 | ip6-trusthost8 | ip6-trusthost9
      | ip6-trusthost10} <address_ipv6mask>
    set password <admin_password>
    set password-expire <date> <time>
    set peer-auth {disable | enable}
    set peer-group <peer-grp>
    set radius-vdom-override {enable | disable}
    set remote-auth {enable | disable}
    set remote-group <name>
    set schedule <schedule-name>
    set sms-phone <cell_phone_number>
    set sms-provider <string>
    set ssh-public-key1 "<key-type> <key-value>"
    set ssh-public-key2 "<key-type> <key-value>"
    set ssh-public-key3 "<key-type> <key-value>"
    set {trusthost1 | trusthost2 | trusthost3 | trusthost4
      | trusthost5 | trusthost6 | trusthost7 | trusthost8
      | trusthost9 | trusthost10} <address_ipv4mask>
    set two-factor {enable | disable}
    set vdom <vdom_name>
    set wildcard {enable | disable}
  config dashboard
    edit <id>
      set widget-type <module_name>
      set column <column_number>
      set sort-by {bandwidth | session}
      set status {close | open}
      set <custom_options>
    end
  config dashboard-tab
    edit <tab_int>
      set columns {1 | 2}
      set name <name_str>
    end
end

```

end

| Variable | Description | Default |
|---|--|------------------------------------|
| accprofile <profile-name> | Enter the name of the access profile to assign to this administrator account. Access profiles control administrator access to FortiGate features. | No default. |
| accprofile-override {enable disable} | Enable authentication server override of the administrator access profile. Note: This redirection will not occur if HTTPS & SSL-VPN are enabled on the same port. | disable |
| allow-remove-admin-session {enable disable} | Disable to prevent other administrators from closing the session. This field is available for accounts with the super_admin profile. | enable |
| comments <comments_string> | Enter the last name, first name, email address, phone number, mobile phone number, and pager number for this administrator. Separate each attribute with a comma, and enclose the string in double-quotes. The total length of the string can be up to 128 characters. (Optional) | null |
| force-password-change {enable disable} | Enable to require this administrator to change password at next login. Disabling this option does not prevent required password change due to password policy violation or expiry. This is available only if password policy is enabled. See “system password-policy” on page 603 . | disable |
| guest-auth {enable disable} | Enable guest authentication. | disable |
| guest-usergroups <groups_list> | Enter the user groups used for guests. | No default. |
| gui-log-display { fortianalyzer fortiguard memory disk } | Select the device from which logs are displayed in the web-based manager. | disk or memory, depending on model |
| {ip6-trusthost1 ip6-trusthost2 ip6-trusthost3 ip6-trusthost4 ip6-trusthost5 ip6-trusthost6 ip6-trusthost7 ip6-trusthost8 ip6-trusthost9 ip6-trusthost10} <address_ipv6mask> | Any IPv6 address and netmask from which the administrator can connect to the FortiGate unit. If you want the administrator to be able to access the FortiGate unit from any address, set the trusted hosts to ::/0. | ::/0 |
| password <admin_password> | Enter the password for this administrator. It can be up to 64 characters in length. | null |
| password-expire <date> <time> | Enter the date and time that this administrator's password expires. Enter zero values for no expiry. Date format is YYYY-MM-DD. Time format is HH:MM:SS. | 0000-00-00 00:00:00 |

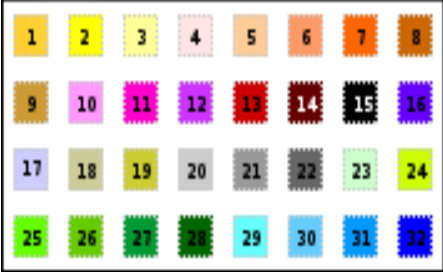
| Variable | Description | Default |
|--|---|-----------------|
| peer-auth {disable enable} | Set to enable peer certificate authentication (for HTTPS admin access). If peer-auth is enabled, two-factor is not available. | disable |
| peer-group <peer-grp> | Name of peer group defined under config user peergrp or user group defined under config user group. Used for peer certificate authentication (for HTTPS admin access). | null |
| radius-vdom-override {enable disable} | Enable RADIUS authentication override for the (wildcard only) administrator. | disable |
| remote-auth {enable disable} | Enable or disable authentication of this administrator using a remote RADIUS, LDAP, or TACACS+ server. | disable |
| remote-group <name> | Enter the administrator user group name, if you are using RADIUS, LDAP, or TACACS+ authentication. This is only available when remote-auth is enabled. | No default. |
| schedule <schedule-name> | Restrict times that an administrator can log in. Defined in config firewall schedule. Null indicates that the administrator can log in at any time. | null |
| sms-phone <cell_phone_number> | Enter the telephone number of the cellular phone where the SMS text message will be sent containing the token code for two-factor authentication. Typically the format does not include the country code, but does include the other digits of the cell phone number. Verify the correct format with the cell phone provider. | null |
| sms-provider <string> | Select an SMS provider from the list of configured entries. This is the cell phone service provider, and the list of providers is configured with the command “system sms-server” on page 679. | No default. |
| ssh-public-key1 "<key-type> <key-value>" | You can specify the public keys of up to three SSH clients. These clients are authenticated without being asked for the administrator password. You must create the public-private key pair in the SSH client application. <key type> is ssh-dss for a DSA key or ssh-rsa for an RSA key. <key-value> is the public key string of the SSH client. | No default. |
| ssh-public-key2 "<key-type> <key-value>" | | No default. |
| ssh-public-key3 "<key-type> <key-value>" | | No default. |
| {trusthost1 trusthost2 trusthost3 trusthost4 trusthost5 trusthost6 trusthost7 trusthost8 trusthost9 trusthost10} <address_ipv4mask> | Any IPv4 address or subnet address and netmask from which the administrator can connect to the FortiGate unit. If you want the administrator to be able to access the FortiGate unit from any address, set the trusted hosts to 0.0.0.0 and the netmask to 0.0.0.0. | 0.0.0.0 0.0.0.0 |

| Variable | Description | Default |
|---|---|---|
| two-factor { enable disable } | Enable to use two-factor authentication with this admin account. When enabled, one of FortiToken, email, or SMS text message to a cellular phone is used as the second factor. | disable |
| vdom <vdom_name> | Enter the name of the VDOM this account belongs to. (Optional) | No default. |
| wildcard { enable disable } | Enable <code>wildcard</code> to allow all accounts on an authentication server to log on to the FortiGate unit as administrator. Disable <code>wildcard</code> if you want to allow only the specified administrator to log on. This is available when <code>remote-auth</code> is enabled. | disable |
| config dashboard variables | | |
| <module_id> | Enter the number of this widget. Use 0 to create a new widget instance. | |
| widget-type <module_name> | Name of the system dashboard or usage widget to configure. For a list of the available widget types, enter: <code>set widget-type ?</code> | No default. |
| column <column_number> | Column in which the dashboard module appears. Values 1 or 2. Available for all dashboard modules. | 0 |
| status {close open} | Set whether the widget is open or closed on the dashboard. | Depends on widget |
| <custom_options> | The custom options for the usage and dashboard widgets are listed in the “Dashboard and usage widget variables” section. | |
| config dashboard-tab variables | | |
| edit <tab_int> | Enter tab number of new dashboard. | No default. |
| columns {1 2} | Select one or two-column format. | 2 |
| name <name_str> | Enter a name for the tab. | No default. |
| Dashboard and usage widget variables | | |
| alert | Configure the information displayed on the alert message console by enabling or disabling the following options: show-admin-auth — admin authentication failures show-amc-bypass — AMC interface bypasses show-conserve-mode — conserve mode alerts show-device-update — device updates show-disk-failure — disk failure alerts show-fds-quota — FortiGuard alerts show-fds-update — FortiGuard updates show-firmware-change — firmware images show-policy-overflow — policy too large (> 64kB) show-power-supply — power supply alerts show-system-restart — system restart alerts | enable enable enable enable enable disable enable enable enable enable |

| Variable | Description | Default |
|-----------|--|---|
| app-usage | <p>Configure the operation of the top application usage widget:</p> <p>display-format {chart table}— display data in a chart or a table.</p> <p>refresh-interval <interval_int> — set the time interval for updating the widget display in the range 10 to 240 seconds or 0 to disable</p> <p>report-by {application destination protocol source}— set the attribute by which to report application usage.</p> <p>resolve-host {disable enable}— display host names (instead of IP addresses).</p> <p>show-auth-use {disable enable}— include the user name of authenticated users.</p> <p>sort-by {bytes msg-counts}— sort information by data (bytes) or number of session (msg-counts).</p> <p>top-n <results_int> — set the number of results to display. The default value displays the top 10 results.</p> <p>vdom <vdom_str> — display results for a specific VDOM.</p> | <p>chart</p> <p>0</p> <p>source</p> <p>disable</p> <p>disable</p> <p>bytes</p> <p>10</p> <p>No default.</p> |
| jsconsole | Set the dashboard column and open and closed status of the CLI console widget. | |
| licinfo | Set the dashboard column and open and closed status of the License information widget. | |

| Variable | Description | Default |
|----------------|--|-----------------------------------|
| protocol-usage | <p>For the top protocol usage widget set the column and open and closed status and set the following options:</p> <p>display-format {chart line}— display data as a bytes-per-protocol bar chart or a color-coded bytes-over-time line graph.</p> <p>protocols <integer> — select the protocols to display by entering the sum of the desired protocol values:</p> <ul style="list-style-type: none"> • 1 Browsing • 2 DNS • 4 Email • 8 FTP • 16 Gaming • 32 Instant Messaging • 64 Newsgroups • 128 P2P • 256 Streaming • 512 TFTP • 1024 VoIP • 2048 Generic TCP • 4096 Generic UDP • 8192 Generic ICMP • 16384 Generic IP <p>time-period — the time period in minutes that the display covers. The default is 1440 (24 hours).</p> | <p>chart</p> <p>0</p> <p>1440</p> |

| Variable | Description | Default |
|---|--|---|
| sessions | <p>For the top session dashboard widget set the dashboard column and open and closed status and set the following options:</p> <p>aggregate-hosts {enable disable} — enable or disable aggregation of hosts in the widget.</p> <p>display-format {chart table} — display data in a chart or a table.</p> <p>dst-interface — set destination interface filter for session display</p> <p>ip-version — set Internet Protocol version of sessions to display: IPv4, IPv6, or ipboth.</p> <p>refresh-interval <interval_int> — set the time interval for updating the widget display in the range 10 to 240 seconds or 0 to disable.</p> <p>sort-by {bytes msg-counts} — sort information by the amount of data (bytes) or the number of session (msg-counts).</p> <p>top-n <results_int> — set the number of results to display. The default value displays the top 10 results.</p> <p>vdom <vdom_str> — display results for a specific VDOM.</p> | <p>chart</p> <p>(null)</p> <p>ipboth</p> <p>0</p> <p>bytes</p> <p>10</p> <p>No default.</p> |
| sessions-history | Set the dashboard column, chart color, and view-type. | |
| show-forward-traffic {enable disable} | Enable or disable display of forward traffic in Sessions widget. Forward traffic is any traffic through the FortiGate that has a policy id. | disable |
| show-local-traffic {enable disable} | Enable or disable display of local traffic in Sessions widget. Local traffic is traffic to/from the FortiGate unit (no policy id). | disable |
| sort-by {bandwidth session} | Choose sort by bandwidth or session for sessions-bandwidth widget. | bytes |
| statistics | Set the dashboard column and open and closed status of the log and archive statistics dashboard widget. | |
| storage | Set the dashboard column and open and closed status of the log and archive storage dashboard widget. | |
| sysinfo | Set the dashboard column and open and closed status of the system information dashboard widget. | |
| sysop | Set the dashboard column and open and closed status of the unit operation dashboard widget. | |

| Variable | Description | Default |
|------------|--|---------|
| sysres | <p>For the system resources dashboard widget set the dashboard column and open and closed status and set the following options:</p> <p>chart-color <color_int> — select the chart color for the historical display. Default is 1.</p>  <p>cpu-display-type {average each} — select display of each core or average of all cores on multicore processor models.</p> <p>view-type {historical real-time} — select historical graph or current value dial display.</p> <p>time-period <minutes_int> — set time period in minutes for historical display</p> | |
| tr-history | <p>For the traffic history dashboard widget set the dashboard column and open and closed status and set the following options:</p> <p>refresh {disable enable} — enable automatically refreshing the display</p> <p>interface <interface_name> — name of interface monitored for traffic history data.</p> <p>tr-history-period1, tr-history-period2, tr-history-period3 — time period (seconds) for each of the three history graphs. To disable a graph, set its period to 0.</p> | |

amc

Use this command to configure AMC ports on your FortiGate unit.

Syntax

```
config system amc
    set {dw1 | dw2} {adm-fb8 | adm-fe8 | adm-xb2 | adm-xd4 | adm-xe2
        | auto | none}
    set {sw1 | sw2} {asm-ce4 | asm-cx4 | asm-disk | asm-fb4 | asm-et4
        | asm-fx2 | auto | none}
end
```

| Variable | Description | Default |
|---|--|---------|
| {dw1 dw2} {adm-fb8 adm-fe8 adm-xb2 adm-xd4 adm-xe2 auto none} | Configure this double width AMC slot for the following type of module. adm-fb8 — AMC double width 8G NP2 accelerated network interface module adm-fe8 — AMC double width 8G FE8 accelerated network interface module adm-xb2 — AMC double width 2XG NP2 accelerated network interface module adm-xd4 — AMC double width 4XG XD4 accelerated network interface module adm-xe2 — AMC double width 2XG XE2 accelerated network interface module auto — support any card that is inserted none — not configured, disable slot | auto |
| {sw1 sw2} {asm-ce4 asm-cx4 asm-disk asm-fb4 asm-et4 asm-fx2 auto none} | Configure this single width AMC port for the following type of card. asm-ce4 — AMC single width, 4G CE4 accelerated network interface module asm-cx4 — AMC single width, 4G bypass asm-disk — AMC Single width SCSI hard disk card, such as ASM-S08 asm-fb4 — AMC single width 4G NP2 accelerated network interface module asm-et4 — AMC single width T1/E1 network interface module asm-fx2 — AMC single width, 2G bypass auto — support any single width card none — not configured, disable slot | auto |

arp-table

Use this command to manually configure add ARP table entries to the FortiGate unit. ARP table entries consist of a interface name, an IP address, and a MAC address.

Limits for the number of ARP table entries are software limits set by the FortiGate configuration as documented in the [FortiGate Maximum Values Matrix](#) document.

This command is available per VDOMs.

Syntax

```
config system arp-table
  edit <table_value>
    set interface <port>
    set ip <address_ipv4>
    set mac <mac_address>
  end
```

| Variable | Description | Default |
|-------------------|---|-------------|
| interface <port> | Enter the interface this ARP entry is associated with | No default |
| ip <address_ipv4> | Enter the IP address of the ARP entry. | No default. |
| mac <mac_address> | Enter the MAC address of the device entered in the table, in the form of xx:xx:xx:xx:xx:xx. | No default. |

auto-install

Use this command to configure automatic installation of firmware and system configuration from a USB disk when the FortiGate unit restarts. This command is available only on units that have a USB disk connection.

If you set both configuration and firmware image update, both occur on the same reboot. The FortiGate unit will not reload a firmware or configuration file that is already loaded.

Third-party USB disks are supported; however, the USB disk must be formatted as a FAT16 drive. No other partition type is supported.

To format your USB Disk when its connected to your FortiGate unit, at the CLI prompt type “`exe usb-disk format`”.

To format your USB disk when it is connected to a Windows system, at the command prompt type “`format <drive_letter>: /FS:FAT /V:<drive_label>`” where `<drive_letter>` is the letter of the connected USB drive you want to format, and `<drive_label>` is the name you want to give the USB disk volume for identification.



This command is available only when a USB key is installed on the FortiGate unit. Formatting your USB disk will delete all information on your USB disk.

Syntax

```
config system auto-install
  set auto-install-config {enable | disable}
  set auto-install-image {enable | disable}
  set default-config-file
  set default-image-file
end
```

| Variable | Description | Default |
|---|---|-----------------|
| auto-install-config {enable disable} | Enable or disable automatic loading of the system configuration from a USB disk on the next reboot. | disable |
| auto-install-image {enable disable} | Enable or disable automatic installation of firmware from a USB disk on the next reboot. | disable |
| default-config-file | Enter the name of the configuration file on the USB disk. | fgt_system.conf |
| default-image-file | Enter the name of the image file on the USB disk. | image.out |

autoupdate push-update

Use this command to configure push updates. The FortiGuard Distribution Network (FDN) can push updates to FortiGate units to provide the fastest possible response to critical situations such as software exploits or viruses. You must register the FortiGate unit before it can receive push updates.

When you configure a FortiGate unit to allow push updates, the FortiGate unit sends a SETUP message to the FDN. The next time an update is released, the FDN notifies all FortiGate units that are configured for push updates that a new update is available. Within 60 seconds of receiving a push notification, the FortiGate unit requests an update from the FDN.

By using this command, you can enable or disable push updates. You can also configure push IP address and port overrides. If the FDN must connect to the FortiGate unit through a NAT device, you must configure port forwarding on the NAT device and add the port forwarding information to the push update override configuration.



You cannot receive push updates through a NAT device if the external IP address of the NAT device is dynamic (for example, set using PPPoE or DHCP).

Syntax

```
config system autoupdate push-update
    set status {enable | disable}
    set override {enable | disable}
    set address <push_ipv4>
    set port <FDN_port>
end
```

| Variable | Description | Default |
|-----------------------------|---|---------|
| status {enable disable} | Enable or disable FDN push updates. | disable |
| override {enable disable} | Enable an override of push updates. Select enable if the FortiGate unit connects to the FDN through a NAT device. | disable |
| address <push_ipv4> | Enter the External IP address that the FDN connects to if you want to enable push override. This is the address of the external interface of your NAT device. | 0.0.0.0 |
| port <FDN_port> | Enter the port that the FDN connects to. This can be port 9443 by default or a different port that you assign. | 9443 |

autoupdate schedule

Use this command to enable or disable scheduled FDN updates at regular intervals throughout the day, once a day, or once a week.

To have your FortiGate unit to update at a random time during a particular hour, select a time that includes 60 minutes as this will choose a random time during that hour for the scheduled update.

Syntax

```
config system autoupdate schedule
    set status {enable | disable}
    set frequency {every | daily | weekly}
    set time <hh:mm>
    set day <day_of_week>
end
```

| Variable | Description | Default |
|---------------------------------------|--|---------|
| status {enable disable} | Enable or disable scheduled updates. | enable |
| frequency {every daily weekly} | Schedule the FortiGate unit to check for updates every hour, once a day, or once a week. Set <code>interval</code> to one of the following: every — Check for updates periodically. Set <code>time</code> to the time interval to wait between updates. daily — Check for updates once a day. Set <code>time</code> to the time of day to check for updates. weekly — Check for updates once a week. Set <code>day</code> to the day of the week to check for updates. Set <code>time</code> to the time of day to check for updates. | every |
| time <hh:mm> | Enter the time at which to check for updates. hh — 00 to 23 mm — 00-59, or 60 for random minute | 00:00 |
| day <day_of_week> | Enter the day of the week on which to check for updates. Enter one of: Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, or Saturday. This option is available only when <code>frequency</code> is set to weekly. | Monday |

autoupdate tunneling

Use this command to configure the FortiGate unit to use a proxy server to connect to the FortiGuard Distribution Network (FDN). You must enable tunneling so that you can use the proxy server, and also add the IP address and port required to connect to the proxy server. If the proxy server requires authentication, add the user name and password required to connect to the proxy server.

The FortiGate unit connects to the proxy server using the HTTP CONNECT method, as described in RFC 2616. The FortiGate unit sends a HTTP CONNECT request to the proxy server (optionally with authentication information) specifying the IP address and port required to connect to the FDN. The proxy server establishes the connection to the FDN and passes information between the FortiGate unit and the FDN.

The CONNECT method is used mostly for tunneling SSL traffic. Some proxy servers do not allow CONNECT to connect to any port; proxy servers restrict the allowed ports to the well known ports for HTTPS and perhaps some other similar services. FortiGate autoupdates use HTTPS on port 8890 to connect to the FDN, so your proxy server may need to be configured to allow connections on this port.

Syntax

```
config system autoupdate tunneling
    set address <proxy_address>
    set password <password>
    set port <proxy_port>
    set status {enable | disable}
    set username <name>
end
```

| Variable | Description | Default |
|---------------------------|--|-------------|
| address <proxy_address> | The IP address or fully qualified domain name of the proxy server. | No default. |
| password <password> | The password to connect to the proxy server if one is required. | No default. |
| port <proxy_port> | The port required to connect to the proxy server. | 0 |
| status {enable disable} | Enable or disable tunneling. | disable |
| username <name> | The user name used to connect to the proxy server. | No default. |

aux

Use this command to configure the AUX port. You can use a modem connected to the AUX port to remotely connect to a console session on the FortiGate unit

The main difference between the standard console port and the AUX port is that the standard console port is for local serial console connections only. An AUX port cannot accept a modem connection to establish a remote console connection. The AUX console port allows you to establish a local connection, but it has some limitations the standard console port does not have.

- The AUX port will not display the booting messages that the standard console connection displays.
- The AUX port will send out modem initializing strings (AT strings) that will appear on an AUX console session at the start.

Syntax

```
config system aux
    set baudrate <baudrate>
end
```

<baudrate> is the speed of the connection. It can be set to one of the following: 9600, 19200, 38400, 57600, or 115200. The default is 9600.

Ensure devices on both ends of the connection are set to the same baudrate.

bug-report

Use this command to configure a custom email relay for sending problem reports to Fortinet customer support.

Syntax

```
config system bug-report
  set auth {no | yes}
  set mailto <email_address>
  set password <password>
  set server <servername>
  set username <name>
  set username-smtp <account_name>
end
```

| Variable | Description | Default |
|------------------------------|---|------------------|
| auth {no yes} | Enter <i>yes</i> if the SMTP server requires authentication or <i>no</i> if it does not. | no |
| mailto <email_address> | The email address for bug reports. The default is <code>bug_report@fortinetvirussubmit.com</code> . | See description. |
| password <password> | If the SMTP server requires authentication, enter the password required. | No default. |
| server <servername> | The SMTP server to use for sending bug report email. The default server is <code>fortinetvirussubmit.com</code> | See description. |
| username <name> | A valid user name on the specified SMTP server. The default user name is <code>bug_report</code> . | See description. |
| username-smtp <account_name> | A valid user name on the specified SMTP server. The default user name is <code>bug_report</code> . | See description. |

bypass

Use this command to configure bypass operation on FortiGate models 600C and 1000C. This is available in transparent mode only.

Syntax

```
config system bypass
  set bypass-timeout {2 | 4 | 6 | 8 | 10 | 12 | 14}
  set bypass-watchdog {enable | disable}
  set poweroff-bypass {enable | disable}
end
```

| Variable | Description | Default |
|---|--|---------|
| bypass-timeout {2 4 6 8 10 12 14} | Set the time in seconds to wait before entering bypass mode after the system becomes unresponsive. | 10 |
| bypass-watchdog {enable disable} | Enable or disable monitoring for bypass condition. | disable |
| poweroff-bypass {enable disable} | Enable bypass function. | disable |



To enable power off bypass, you must enable both `bypass-watchdog` and `poweroff-bypass`.

central-management

Use this command to configure a central management server for this FortiGate unit. Central management uses a remote server to backup, restore configuration, and monitor the FortiGate unit. The remote server can be either a FortiManager or a FortiGuard server.

This command replaces the `config system fortimanager` command from earlier versions.

Syntax

```
config system central-management
    set mode {normal | backup}
    set type {fortiguard | fortimanager }
    set schedule-config-restore {enable | disable}
    set schedule-script-restore {enable | disable}
    set allow-monitor {enable | disable}
    set allow-push-configuration {enable | disable}
    set allow-pushd-firmware {enable | disable}
    set allow-remote-firmware-upgrade {enable | disable}
    set enc-algorithm {default | high | low}
    set fortimanager-fds-override {enable | disable}
    set fmg <fmg_ipv4>
    set fmg-source-ip <address_ipv4>
    set use-elbc-vdom {enable | disable}
    set vdom <name_string>
end
```

| Variable | Description | Default |
|---|--|--------------|
| mode {normal backup} | Select the mode: normal — normal central management mode backup — backup central management mode | normal |
| type {fortiguard fortimanager } | Select the type of management server as one of - fortiguard or fortimanager. You can enable remote management from a FortiManager unit or the FortiGuard Analysis and Management Service. | fortimanager |
| schedule-config-restore {enable disable} | Select to enable scheduling the restoration of your FortiGate unit's configuration. | enable |
| schedule-script-restore {enable disable} | Select to enable the restoration of your FortiGate unit's configuration through scripts. | enable |
| allow-monitor {enable disable} | Select to allow the remote service to monitor your FortiGate unit. | enable |
| allow-push- configuration {enable disable} | Select to enable firmware image push updates for your FortiGate unit. | enable |
| allow-pushd-firmware {enable disable} | Select to enable push firmware. | enable |
| allow-remote-firmware- upgrade {enable disable} | Select to allow the remote service to upgrade your FortiGate unit with a new firmware image. | enable |

| Variable | Description | Default |
|---|--|---------|
| enc-algorithm { default high low } | <p>Set encryption strength for communications between the FortiGate unit and FortiManager or FortiAnalyzer.</p> <p>high — 128-bit and larger key length algorithms: DHE-RSA-AES256-SHA, AES256-SHA, EDH-RSA-DES-CBC3-SHA, DES-CBC3-SHA, DES-CBC3-MD5, DHE-RSA-AES128-SHA, AES128-SHA</p> <p>low — 64-bit or 56-bit key length algorithms without export restrictions: EDH-RSA-DES-CBC-SHA, DES-CBC-SHA, DES-CBC-MD5</p> <p>default — high strength algorithms and these medium-strength 128-bit key length algorithms: RC4-SHA, RC4-MD5, RC4-MD</p> | default |
| fmg <fmg_ipv4> | Enter the IP address or FQDN of the remote FortiManager server. | null |
| fmg-source-ip <address_ipv4> | Enter the source IP address to use when connecting to FortiManager. | null |
| fortimanager-fds-override { enable disable } | Enable global FortiManager override of FortiGuard service. | disable |
| use-elbc-vdom { enable disable } | When enabled, FortiManager manages FortiGate through config sync vdom interface. | disable |
| vdom <name_string> | <p>Enter the name of the vdom to use when communicating with the FortiManager unit.</p> <p>This field is optional.</p> | root |

console

Use this command to set the console command mode, the number of lines displayed by the console, and the baud rate.



If this FortiGate unit is connected to a FortiManager unit running scripts, `output` must be set to `standard` for scripts to execute properly.

Syntax

```
config system console
  set baudrate <speed>
  set login {enable | disable}
  set mode {batch | line}
  set output {standard | more}
end
```

| Variable | Description | Default |
|--------------------------|--|---------|
| baudrate <speed> | Set the console port baudrate. Select one of 9600, 19200, 38400, 57600, or 115200. | 9600 |
| login {enable disable} | Enable or disable logon via console. | enable |
| mode {batch line} | Set the console mode to line or batch. Used for autotesting only. | line |
| output {standard more} | Set console output to standard (no pause) or more (pause after each screen is full, resume on keypress). This setting applies to <code>show</code> or <code>get</code> commands only. | more |

ddns

Use this command to configure Dynamic Domain Name Service. If an interface of your FortiGate unit uses a dynamic IP address, you can arrange with a DDNS service to provide a domain name from which traffic is redirected to your network. The DDNS service is updated whenever the IP address changes.

DDNS is available only in NAT/Route mode.

Syntax

```
config system ddns
  edit <index_int>
    set ddns-auth {tsig | disable}
    set ddns-key <base64_str>
    set ddns-keyname <keyname_str>
    set ddns-domain <ddns_domain_name>
    set ddns-password <ddns_password>
    set ddns-server-ip <ipv4_addr>
    set ddns-sn <serno_str>
    set ddns-server <ddns_service>
    set ddns-ttl <ttl_int>
    set ddns-username <ddns_username>
    set ddns-zone <zone_str>
    set monitor-interface <interfaces>
  end
```

| Variable | Description | Default |
|--------------------------------|--|-------------|
| <index_int> | Enter the unique index number for this DDNS entry. | |
| ddns-auth {tsig disable} | Enable TSIG authentication for the generic DDNS server. | disable |
| ddns-key <base64_str> | DDNS update key in base 64 encoding. Available when ddns-auth is tsig. | No default. |
| ddns-keyname <keyname_str> | DDNS update keyname. Available when ddns-auth is tsig. | No default. |
| ddns-domain <ddns_domain_name> | Enter the fully qualified domain name to use for the DDNS. This is the domain name you have registered with your DDNS. This field is available for some DDNS service providers. | No default. |
| ddns-password <ddns_password> | Enter the password to use when connecting to the DDNS server. This is not available when ddns-server is dipdns.net. | No default. |
| ddns-server-ip <ipv4_addr> | Enter the DDNS server IP address for generic DDNS server. | 0.0.0.0 |
| ddns-sn <serno_str> | Enter the DDNS serial number (dipdns.net). | No default. |

| Variable | Description | Default |
|-----------------------------------|--|-------------|
| ddns-server <ddns_service> | <p>Select a DDNS server to use. The client software for these services is built into the FortiGate firmware. The FortiGate unit can only connect automatically to a DDNS server for these supported clients.</p> <p>dhs.org — supports members.dhs.org and dnsalias.com.</p> <p>dipdns.net — supports dipdnsserver.dipdns.com.</p> <p>dyndns.org — supports members.dyndns.org.</p> <p>dyns.net — supports www.dyns.net.</p> <p>easydns.com — supports members.easydns.com.</p> <p>FortiGuardDDNS — supports FortiGuard DDNS service.</p> <p>genericDDNS — supports DDNS server (RFC 2136) defined in ddns-server-ip.</p> <p>now.net.cn — supports ip.todayisp.com.</p> <p>ods.org — supports ods.org.</p> <p>tzo.com — supports rh.tzo.com.</p> <p>vavic.com — supports ph001.oray.net(Peanut Hull).</p> | No default. |
| ddns-ttl <ttl_int> | Enter the time-to-live value for DDNS packets. | 300 |
| ddns-username <ddns_username> | <p>Enter the user name to use when connecting to the DDNS server.</p> <p>This is not available when ddns-server is dipdns.net.</p> | No default. |
| ddns-zone <zone_str> | Enter a name for your DDNS zone. Available if ddns-server is genericDDNS. | No default. |
| monitor-interface <interfaces> | Select the network interfaces that use DDNS service. | No default. |

dedicated-mgmt

Use this command to configure the dedicated management port. This port is in the hidden VDOM dmgmt-vdom, which cannot be made the management VDOM. Therefore, the dedicated management port supports CLI access for configuration but does not permit management traffic such as firmware update or unit registration.

Syntax

```
config system dedicated-mgmt
  set status {enable | disable}
  set default-gateway <IPv4_addr>
  set dhcp-server {enable | disable}
  set interface <port_name>
end
```

| Variable | Description | Default |
|--------------------------------|--|-------------|
| status {enable disable} | Enable dedicated management port. | enable |
| default-gateway <IPv4_addr> | Enter the default gateway address. | 192.168.1.1 |
| dhcp-server {enable disable} | Enable or disable the DHCP server for the management port. | disable |
| interface <port_name> | Enter the interface to be used for management. | mgmt |

dhcp reserved-address

Use this command to reserve an IP address for a particular client identified by its device MAC address and type of connection. The DHCP server then always assigns the reserved IP address to the client. You can define up to 200 reserved addresses.



This command is deprecated. Use the `config reserved-address` subcommand of the `system dhcp server` command instead.



For this configuration to take effect, you must configure at least one DHCP server using the `config system dhcp server` command, see “[system dhcp server](#)” on page 501.

Syntax

```
config system dhcp reserved-address
  edit <id_int>
    set ip <address_ipv4>
    set mac <address_hex>
    set type {regular | ipsec}
  end
```

| Variable | Description | Default |
|------------------------|---|-------------------|
| ip <address_ipv4> | Enter the IPv4 address. | 0.0.0.0 |
| mac <address_hex> | Enter the MAC address. | 00:00:00:00:00:00 |
| type {regular ipsec} | Enter the type of the connection to be reserved: regular — Client connecting through regular Ethernet ipsec — Client connecting through IPSec VPN | regular |

dhcp server

Use this command to add one or more DHCP servers for any FortiGate interface. As a DHCP server, the interface dynamically assigns IP addresses to hosts on a network connected to the interface.

You can use the `config system dhcp reserved` command to reserve an address for a specific MAC address. For more information see [“system dhcp reserved-address” on page 500](#).

This command is available only in NAT/Route mode.

Syntax

```
config system dhcp server
  edit <server_index_int>
    set status {enable | disable}
    set auto-configuration {enable | disable}
    set conflicted-ip-timeout <timeout_int>
    set default-gateway <address_ipv4>
    set dns-server1 <address_ipv4>
    set dns-server2 <address_ipv4>
    set dns-server3 <address_ipv4>
    set dns-service {default | specify | local}
    set domain <domain_name_str>
    set interface <interface_name>
    set ip-mode {range | usrgroup}
    set ipsec-lease-hold <release_seconds>
    set lease-time <seconds>
    set mac-acl-default-action {assign | block}
    set netmask <mask>
    set ntp-server1 <ipv4_addr>
    set ntp-server2 <ipv4_addr>
    set ntp-server3 <ipv4_addr>
    set ntp-service {default | specify | local}
    set option1 <option_code> [<option_hex>]
    set option2 <option_code> [<option_hex>]
    set option3 <option_code> [<option_hex>]
    set option4 <option_code> [<option_hex>]
    set option5 <option_code> [<option_hex>]
    set option6 <option_code> [<option_hex>]
    set server-type {ipsec | regular}
    set start-ip <address_ipv4>
    set vci-match {enable | disable}
    set vci-string <string>
    set wifi-ac1 <ipv4_addr>
    set wifi-ac2 <ipv4_addr>
    set wifi-ac3 <ipv4_addr>
    set wins-server1 <wins_ipv4>
    set wins-server2 <wins_ipv4>
    set wins-server3 <wins_ipv4>
```

```

config exclude-range
    edit <excl_range_int>
        set end-ip <end_ipv4>
        set start-ip <start_ipv4>
config ip-range
    edit <ip_range_int>
        set end-ip <address_ipv4>
        set start-ip <address_ipv4>
config reserved-address
    edit <id_int>
        set action {assign | block | reserved}
        set description <desc_str>
        set ip <ipv4_addr>
        set mac <mac_addr>
end
end

```

| Variable | Description | Default |
|--|---|---------|
| edit <server_index_int> | Enter an integer ID for the DHCP server. The sequence number may influence routing priority in the FortiGate unit forwarding table. | |
| status {enable disable} | Enable or disable this DHCP server. | enable |
| auto-configuration {enable disable} | Enable or disable automatic configuration. | enable |
| conflicted-ip-timeout <timeout_int> | Enter the time in seconds to wait after a conflicted IP address is removed from the DHCP range before it can be reused. Valid range is from 60 to 8640000 seconds (1 minute to 100 days). | 1800 |
| default-gateway <address_ipv4> | The IP address of the default gateway that the DHCP server assigns to DHCP clients. | 0.0.0.0 |
| dns-server1 <address_ipv4> | The IP address of the first DNS server that the DHCP server assigns to DHCP clients. Used if <code>dns-service</code> is set to <code>specify</code> . | 0.0.0.0 |
| dns-server2 <address_ipv4> | The IP address of the second DNS server that the DHCP server assigns to DHCP clients. Used if <code>dns-service</code> is set to <code>specify</code> . | 0.0.0.0 |
| dns-server3 <address_ipv4> | The IP address of the third DNS server that the DHCP server assigns to DHCP clients. Used if <code>dns-service</code> is set to <code>specify</code> . | 0.0.0.0 |
| dns-service {default specify local} | Select <code>default</code> to assign DHCP clients the DNS servers added to the FortiGate unit using the <code>config system dns</code> command. Select <code>specify</code> to specify the DNS servers that this DHCP server assigns to DHCP clients. Use the <code>dns-server#</code> options to add DNS servers to this DHCP server configuration. Select <code>local</code> to use this FortiGate unit as a DNS server. | specify |
| domain <domain_name_str> | Domain name suffix for the IP addresses that the DHCP server assigns to DHCP clients. | |

| Variable | Description | Default |
|--|---|---------------------------------------|
| interface <interface_name> | The FortiGate unit interface that this DHCP server can assign IP addresses from. Devices connected to this interface can get their IP addresses from this DHCP server. You can only add one DHCP server to an interface. | |
| ip-mode {range usrgrp} | Configure whether an IPsec DHCP server assigns IP addresses based on the IP address range added to the configuration or based on the user group of the IPsec VPN user. Visible only when <code>server-type</code> is set to <code>ipsec</code> . | range |
| ipsec-lease-hold <release_seconds> | Set the DHCP lease release delay in seconds for DHCP-over-IPSec tunnels when the tunnel goes down. A value of 0 disables the forced expiry of the DHCP-over-IPSec leases. Visible only when <code>server-type</code> is set to <code>ipsec</code> . | 60 |
| lease-time <seconds> | The interval in seconds after which a DHCP client must ask the DHCP server for new settings. The lease duration must be between 300 and 864,000 seconds (10 days). Set <code>lease-time</code> to 0 for an unlimited lease time. | 604800 (7 days) |
| mac-acl-default-action {assign block} | MAC access control default action. | assign |
| netmask <mask> | The DHCP client netmask assigned by the DHCP server. | 0.0.0.0 |
| ntp-server1 <ipv4_addr> ntp-server2 <ipv4_addr> ntp-server3 <ipv4_addr> | The IP addresses of up to three NTP servers. | 0.0.0.0 0.0.0.0 0.0.0.0 |
| ntp-service {default specify local} | Select <code>default</code> to use system NTP settings. Select <code>specify</code> to specify the NTP servers that this DHCP server assigns to DHCP clients. Use the <code>ntp-server#</code> options to add NTP servers to this DHCP server configuration. Select <code>local</code> to use this FortiGate unit as an NTP server. | specify |

| Variable | Description | Default |
|--|---|-------------------------------|
| option1 <option_code> [<option_hex>] option2 <option_code> [<option_hex>] option3 <option_code> [<option_hex>] option4 <option_code> [<option_hex>] option5 <option_code> [<option_hex>] option6 <option_code> [<option_hex>] | The DHCP server can send up to six custom DHCP options. <code>option_code</code> is the DHCP option code in the range 1 to 255. <code>option_hex</code> is an even number of hexadecimal characters. For detailed information about DHCP options, see RFC 2132, DHCP Options and BOOTP Vendor Extensions. | 0 |
| server-type {ipsec regular} | Enter the type of client to serve: regular client connects through regular Ethernet ipsec client connects through IPsec VPN | regular |
| vci-match {enable disable} | Enable to turn on vendor class identifier (VCI) matching. When enabled only DHCP requests with the matching VCI string will be served. | disable |
| vci-string <string> | Enter the VCI names to match when <code>vci-match</code> is enabled. Separate strings with spaces. | No default. |
| wifi-ac1 <ipv4_addr> wifi-ac2 <ipv4_addr> wifi-ac3 <ipv4_addr> | The IP addresses of up to three WiFi controllers. | 0.0.0.0 0.0.0.0 0.0.0.0 |
| wins-server1 <wins_ipv4> | The IP address of the first WINS server that the DHCP server assigns to DHCP clients. | 0.0.0.0 |
| wins-server2 <wins_ipv4> | The IP address of the second WINS server that the DHCP server assigns to DHCP clients. | 0.0.0.0 |
| wins-server3 <wins_ipv4> | The IP address of the third WINS server that the DHCP server assigns to DHCP clients. | 0.0.0.0 |
| config exclude-range fields | | |
| edit <excl_range_int> | Enter an integer ID for this exclusion range. Configure a range of IP addresses to exclude from the list of DHCP addresses that are available. You can add up to 16 exclusion ranges of IP addresses that the FortiGate DHCP server cannot assign to DHCP clients. | No default. |
| end-ip <end_ipv4> | The end IP address in the exclusion range. The start IP and end IP must be in the same subnet. | 0.0.0.0 |
| start-ip <start_ipv4> | The start IP address in the exclusion range. The start IP and end IP must be in the same subnet. | 0.0.0.0 |
| config ip-range fields | | |

| Variable | Description | Default |
|---------------------------------------|--|-------------------|
| edit <ip_range_int> | Enter an integer ID for this IP address range. Configure the range of IP addresses that this DHCP server can assign to DHCP clients. You can add up to 16 ranges of IP addresses that the FortiGate DHCP server can assign to DHCP clients. | No default. |
| end-ip <address_ipv4> | The end IP in the IP addresses range that this DHCP server assigns to DHCP clients. The IP range is defined by the <code>start-ip</code> and the <code>end-ip</code> fields which should both be in the same subnet. | 0.0.0.0 |
| start-ip <address_ipv4> | The starting IP for the range of IP addresses that this DHCP server assigns to DHCP clients. The IP range is defined by the <code>start-ip</code> and the <code>end-ip</code> fields which should both be in the same subnet. | 0.0.0.0 |
| config reserved-address fields | | |
| edit <id_int> | Enter an ID number for this IP address entry. Configure one or more IP addresses that are reserved. These addresses cannot be given out by the DHCP server. There can be a maximum of 16 entries. | No default. |
| action {assign block reserved} | Assign, block, or reserve an IP address. | reserved |
| description <desc_str> | Optionally, enter a description for the host. | |
| ip <ipv4_addr> | Enter an IP address to reserve. It will be bound to this MAC address. | 0.0.0.0 |
| mac <mac_addr> | Enter a MAC address that will be bound to this IP address. If this MAC address comes up in the DHCP list, it will be ignored. | 00:00:00:00:00:00 |

dhcp6 server

Use this command to add one or more IPv6 DHCP servers for any FortiGate interface. As a DHCP server, the interface dynamically assigns IP addresses to hosts on a network connected to the interface.

This command is available in NAT/Route mode only.

Syntax

```
config system dhcp6 server
  edit <server_index_int>
    set status {enable | disable}
    set dns-service {default | specify}
    set dns-server1 <address_ipv6>
    set dns-server2 <address_ipv6>
    set dns-server3 <address_ipv6>
    set domain <domain_name_str>
    set interface <interface_name>
    set lease-time <seconds>
    set option1 <option_code> [<option_hex>]
    set option2 <option_code> [<option_hex>]
    set option3 <option_code> [<option_hex>]
    set subnet <mask>
  config ip-range
    edit <ip_range_int>
      set start-ip <address_ipv6>
      set end-ip <end_ipv6>
    end
  end
```

| Variable | Description | Default |
|---------------------------------|--|---------|
| edit <server_index_int> | Enter an integer ID for the DHCP server. The sequence number may influence routing priority in the FortiGate unit forwarding table. | |
| status {enable disable} | Enable or disable this DHCP server. | enable |
| dns-service {default specify} | Select default to assign DHCP clients the DNS servers added to the FortiGate unit using the <code>config system dns</code> command. Select <code>specify</code> to specify the DNS servers that this DHCP server assigns to DHCP clients. Use the <code>dns-server#</code> options to add DNS servers to this DHCP server configuration. | specify |
| dns-server1 <address_ipv6> | The IP address of the first DNS server that the DHCP server assigns to DHCP clients. Used if <code>dns-service</code> is set to <code>specify</code> . | :: |
| dns-server2 <address_ipv6> | The IP address of the second DNS server that the DHCP server assigns to DHCP clients. Used if <code>dns-service</code> is set to <code>specify</code> . | :: |
| dns-server3 <address_ipv6> | The IP address of the third DNS server that the DHCP server assigns to DHCP clients. Used if <code>dns-service</code> is set to <code>specify</code> . | :: |

| Variable | Description | Default |
|---|---|--------------------|
| domain <domain_name_str> | Domain name suffix for the IP addresses that the DHCP server assigns to DHCP clients. | null |
| interface <interface_name> | The FortiGate unit interface that this DHCP server can assign IP addresses from. Devices connected to this interface can get their IP addresses from this DHCP server. You can only add one DHCP server to an interface. | null |
| lease-time <seconds> | The interval in seconds after which a DHCP client must ask the DHCP server for new settings. The lease duration must be between 300 and 864,000 seconds (10 days). Set <code>lease-time</code> to 0 for an unlimited lease time. | 604800 (7 days) |
| option1 <option_code> [<option_hex>] option2 <option_code> [<option_hex>] option3 <option_code> [<option_hex>] | The first, second, and third custom DHCP options that can be sent by the DHCP server. <code>option_code</code> is the DHCP option code in the range 1 to 255. <code>option_hex</code> is an even number of hexadecimal characters. For detailed information about DHCP options, see RFC 2132, DHCP Options and BOOTP Vendor Extensions. | 0 |
| subnet <mask> | The DHCP client netmask assigned by the DHCP server. | ::/0 |
| config ip-range | Configure the range of IP addresses that this DHCP server can assign to DHCP clients. | |
| edit <ip_range_int> | Enter an integer ID for this IP address range. You can add up to 16 ranges of IP addresses that the FortiGate DHCP server can assign to DHCP clients. | |
| start-ip <address_ipv6> | The starting IP for the range of IP addresses that this DHCP server assigns to DHCP clients. The IP range is defined by the <code>start-ip</code> and the <code>end-ip</code> fields which should both be in the same subnet. | :: |
| end-ip <end_ipv6> | The end IP address for the range of IP addresses that this DHCP server assigns to DHCP clients. The IP range is defined by the <code>start-ip</code> and the <code>end-ip</code> fields which should both be in the same subnet. | :: |

dns

Use this command to set the DNS server addresses. Several FortiGate functions, including sending email alerts and URL blocking, use DNS.

Syntax

```
config system dns
    set cache-notfound-responses {enable | disable}
    set dns-cache-limit <integer>
    set dns-cache-ttl <int>
    set domain <domain_name>
    set ip6-primary <dns_ipv6>
    set ip6-secondary <dns_ip6>
    set primary <dns_ipv4>
    set secondary <dns_ip4>
    set source-ip <ipv4_addr>
end
```

| Variable | Description | Default |
|---|---|---------------|
| cache-notfound-responses {enable disable} | Enable to cache NOTFOUND responses from the DNS server. | disable |
| dns-cache-limit <integer> | Set maximum number of entries in the DNS cache. | 5000 |
| dns-cache-ttl <int> | Enter the duration, in seconds, that the DNS cache retains information. | 1800 |
| domain <domain_name> | Set the local domain name (optional). | No default. |
| ip6-primary <dns_ipv6> | Enter the primary IPv6 DNS server IP address. | :: |
| ip6-secondary <dns_ip6> | Enter the secondary IPv6 DNS server IP address. | :: |
| primary <dns_ipv4> | Enter the primary DNS server IP address. | 208.91.112.53 |
| secondary <dns_ip4> | Enter the secondary DNS IP server address. | 208.91.112.52 |
| source-ip <ipv4_addr> | Enter the IP address for communications to DNS server. | 0.0.0.0 |

dns-database

Use this command to configure the FortiGate DNS database so that DNS lookups from an internal network are resolved by the FortiGate DNS database. To configure the DNS database you add zones. Each zone has its own domain name.

You then add entries to each zone. An entry is an host name and the IP address it resolves to. You can also specify if the entry is an IPv4 address (A), an IPv6 address (AAAA), a name server (NS), a canonical name (CNAME), or a mail exchange (MX) name.

Syntax

```
config system dns-database
    edit <zone-string>
        set allow-transfer <ipv4_addr>
        set authoritative {enable | disable}
        set contact <email_string>
        set domain <domain>
        set forwarder <ipv4_addr>
        set ip-master <ipv4_addr>
        set primary-name <name_string>
        set source-ip <ipv4_addr>
        set status {enable | disable}
        set ttl <int>
        set type {master | slave}
        set view {public | shadow}
    config dns-entry
        edit <entry-id>
            set canonical-name <canonical_name_string>
            set hostname <hostname_string>
            set ip <ip_address>
            set ipv6 <ipv6_address>
            set preference <preference_value>
            set status {enable | disable}
            set ttl <entry_ttl_value>
            set type {A | AAAA | MX | NS | CNAME}
        end
    end
end
```

| Variable | Description | Default |
|----------------------------------|---|-------------|
| edit <zone-string> | Enter the DNS zone name. This is significant only on the FortiGate unit itself. | No default. |
| allow-transfer <ipv4_addr> | DNS zone transfer ip address list. | No default. |
| authoritative {enable disable} | Enable to declare this as an authoritative zone. | enable |
| contact <email_string> | Enter the email address of the administrator for this zone. If the email address is in this zone, you can enter just the username portion of the email address. | hostmaster |
| domain <domain> | Set the domain name here — when matching lookup, use this zone name to match DNS queries. | No default. |

| Variable | Description | Default |
|---|--|-------------|
| forwarder <ipv4_addr> | Enter the ip address of the dns zone forwarder. | No default. |
| ip-master <ipv4_addr> | Enter the IP address of the master DNS server. This is available when <code>type</code> is <code>slave</code> . | No default |
| primary-name <name_string> | Enter the domain name of the default DNS server for this zone. | dns |
| source-ip <ipv4_addr> | Enter the source IP address to use when forwarding to the DNS server. | 0.0.0.0 |
| status {enable disable} | Select to enable this DNS zone entry. | enable |
| ttl <int> | Set the packet time-to-live in seconds. Range 0 to 2 147 483 647. | 86400 |
| type {master slave} | Select the type of this zone. <code>master</code> — manage entries directly. <code>slave</code> — import entries from outside source | master |
| view {public shadow} | Select the type of view for this zone: public — to service public clients shadow — to service internal clients This value cannot be changed once set. This setting can be used in conjunction with config system dns-server entries, where the mode of a zone can be set to recursive. A recursive mode on a zone means DNS requests sent to the FortiGate will first check the Shadow DNS Database and if no entry is found, will then forward to the system DNS setting. | shadow |
| config dns-entry variables | | |
| edit <entry-id> | | |
| canonical-name <canonical_name_string> | Enter the canonical name of the host. This is available if <code>type</code> is <code>CNAME</code> . | Null |
| hostname <hostname_string> | Enter the name of the host. | Null |
| ip <ip_address> | Enter the IP address (IPv4) of the host. This is available if <code>type</code> is <code>A</code> . | 0.0.0.0 |
| ipv6 <ipv6_address> | Enter the IP address (IPv6) of the host. This is available if <code>type</code> is <code>AAAA</code> . | :: |
| preference <preference_value> | Enter the preference level. 0 is the highest preference. This is available if <code>type</code> is <code>MX</code> . | 10 |
| status {enable disable} | Enable the DNS entry. | enable |

| Variable | Description | Default |
|--|--|---------|
| <code>ttl <entry_ttl_value></code> | Optionally, override the zone time-to-live value. Range 0 to 2 147 483 647 seconds. Set to 0 to use zone <code>ttl</code> value. | 0 |
| <code>type {A AAAA MX NS CNAME}</code> | A — IPv4 host AAAA — IPv6 host CNAME — alias MX — mail server NS — name server | A |

dns-server

Use this command to configure the dns-server on a particular interface.

Syntax

```
config system dns-server
edit <intf_name>
    set mode {forward-only | non-recursive | recursive}
end
```

| Variable | Description | Default |
|---|---|-----------|
| mode {forward-only non-recursive recursive} | Select the mode the dns-server for this interface will use. forward-only — Forward query to the DNS server configured for the FortiGate unit. non-recursive — Look up domain name in local database. Do not relay the request to the DNS server configured for the FortiGate unit. See system dns-database on page 367. recursive — Look up domain name in local database. If the entry is not found, relay the request to the DNS server configured for the FortiGate unit. | recursive |

elbc

Use this command to set the chassis load balancing (ELBC) information for the FortiOS unit. Unit must be in Transparent mode.

A FortiTrunk is a group of backplane slots where the fabric can load balance traffic. In order for this to happen, the trunk members (the blades) are responsible for sending their heartbeats over the fabric channel to the FortiSwitch. If blades are standalone each sends a heartbeat, but if they are in a FGCP HA cluster, only one heart beat is sent and the load balanced traffic is forwarded to the primary HA unit.

Syntax

```
config system elbc
    set mode {none | content-cluster | dual-forticontroller
              | forticontroller | forti-trunk | service-group}
    set graceful-upgrade {enable | disable}
    set hb-device <intf_name>
    set inter-chassis-support {enable | disable}
end
```

| Variable | Description | Default |
|---|--|-------------|
| mode {none content-cluster dual-forticontroller forticontroller forti-trunk service-group} | Select the ELBC mode to use. <ul style="list-style-type: none"> • none — no ELBC operation • content-cluster — load balance UTM traffic • forticontroller — FortiController • forti-trunk — use the FortiTrunk feature. • service-group — full support of enhanced load balance cluster | none |
| graceful-upgrade {enable disable} | Enable to upgrade the HA cluster when using ELBCv3. It will upgrade the primary unit after first upgrading the other units in the cluster. | enable |
| hb-device <intf_name> | Specify the heartbeat interface for FortiTrunk mode. | No default. |
| inter-chassis-support {enable disable} | Enable or disable content cluster (aka. HAoC) inter-chassis support. When enabled, B1 and B2 on the FSW-5203B will become a static link-aggregate, and will be used as HA hbdevs. FSW-5203B within a chassis cannot use the switch inter-connect as an HA hbdev when "inter-chassis-support" is enabled, and must be connected via B1/B2 instead. Disabling "inter-chassis-support" destroys the link-aggregate and resumes using the switch interconnect as the HA hbdev. | disable |

email-server

Use this command to configure the FortiGate unit to access an SMTP server to send alert emails. This command is global in scope.

Syntax

```
config system email-server
    set authenticate {enable | disable}
    set password <password_str>
    set port <port_integer>
    set reply-to <reply-to_str>
    set security {none | smtps | starttls}
    set server {<name-str> | <address_ipv4>}
    set source-ip <address_ipv4>
    set source-ip6 <address_ipv6>
    set username <username_str>
end
```

| Variable | Description | Default |
|---|--|-------------|
| authenticate {enable disable} | Enable SMTP authentication if the FortiGate unit is required to authenticate before using the SMTP server. This field is accessible only if <code>type</code> is <code>custom</code> and <code>server</code> is defined. | disable |
| password <password_str> | Enter the password that the FortiGate unit needs to access the SMTP server. This field is accessible only if <code>type</code> is <code>custom</code> , <code>authenticate</code> is enabled and <code>server</code> is defined. | No default. |
| port <port_integer> | Change the TCP port number that the FortiGate unit uses to connect to the SMTP server. The standard SMTP port is 25. You can change the port number if the SMTP server has been configured to use a different port. | 25 |
| reply-to <reply-to_str> | Optionally, specify the reply-to email address. | No default. |
| security {none smtps starttls} | Select the security profile to use for email. | none |
| server {<name-str> <address_ipv4>} | Enter the name of the SMTP server, in the format <code>smtp.domain.com</code> , to which the FortiGate unit should send email. Alternately, the IP address of the SMTP server can be entered. The SMTP server can be located on any network connected to the FortiGate unit. | No default. |
| source-ip <address_ipv4> | Enter the SMTP server source IPv4 address. | No default. |
| source-ip6 <address_ipv6> | Enter the SMTP server source IPv6 address. | No default. |
| username <username_str> | Enter the user name for the SMTP server that the FortiGate unit uses to send alert emails. This variable is accessible only if <code>authenticate</code> is enabled and <code>server</code> is defined. | No default. |

fips-cc

Use this command to set the FortiGate unit into FIPS-CC mode.

Enable Federal Information Processing Standards-Common Criteria (FIPS-CC) mode. This is an enhanced security mode that is valid only on FIPS-CC-certified versions of the FortiGate firmware.

When switching to FIPS-CC mode, you will be prompted to confirm, and you will have to login.



When you enable FIPS-CC mode, all of the existing configuration is lost.

Syntax

```
config system fips-cc
  set entropy-token {enable | disable | dynamic}
  set status {enable | disable}
end
```

| Variable | Description | Default |
|--|--|---------|
| entropy-token {enable disable dynamic} | Set use of FortiTRNG token at boot-up in FIPS-CC mode: enable — token required disable — token not required dynamic — token used if present | dynamic |
| status {enable disable} | Enable to select FIPS-CC mode operation for the FortiGate unit. | disable |

fortiguard

Use this command to configure communications with the FortiGuard Distribution Network (FDN) for FortiGuard subscription services such as:

- FortiGuard Antivirus and IPS
- FortiGuard Web Filtering and Antispam
- FortiGuard Analysis and Management Service
- FortiGuard DNS-based web filtering

For FortiGuard Antivirus and IPS, Web Filtering and Antispam, you can alternatively use this command to configure the FortiGate unit to communicate with a FortiManager system, which can act as a private FortiGuard Distribution Server (FDS) for those services.

By default, FortiGate units connect to the FDN using a set of default connection settings. You can override these settings to use IP addresses and port numbers other than the defaults. For example, if you have a FortiManager unit, you might download a local copy of FortiGuard service updates to the FortiManager unit, then redistribute those updates by configuring each FortiGate unit's server override feature to connect to the FortiManager unit's private FDS IP address.



If the FortiGate unit is unable to connect to the FDN, verify connectivity on required ports. For a list of required ports, see the Fortinet Knowledge Center article [Traffic Types and TCP/UDP Ports Used by Fortinet Products](#).

Remote administration by a FortiManager system is mutually exclusive with remote administration by FortiGuard Analysis and Management Service. For information about configuring remote administration by a FortiManager system instead, see “[system central-management](#)” on page 494.

Syntax

```
config system fortiguard
  set port {53 | 8888}
  set ddns-server-ip <IPv4_addr>
  set ddns-server-port <port_int>
  set service-account-id <id_str>
  set service-account-passwd <pwd_str>
  set load-balance-servers <number>
  set antispam-cache {enable | disable}
  set antispam-cache-ttl <ttl_int>
  set antispam-cache-mpercent <ram_int>
  set antispam-expiration
  set antispam-force-off {enable | disable}
  set antispam-license
  set antispam-timeout <timeout_int>
  set avquery-cache {enable | disable}
  set avquery-cache-ttl <ttl_int>
  set avquery-cache-mpercent <max_int>
  set avquery-force-off {enable | disable}
  set avquery-license
```

```

set avquery-expiration
set avquery-timeout <timeout_int>
set webfilter-cache {enable | disable}
set webfilter-cache-ttl <tll_int>
set webfilter-expiration
set webfilter-force-off {enable | disable}
set webfilter-license
set webfilter-sdns-server-ip
set webfilter-sdns-server-port
set webfilter-timeout <timeout_int>
end

```

| Variable | Description | Default |
|--------------------------------------|--|-------------|
| port {53 8888} | Enter the port to use for rating queries to the FortiGuard Web Filtering or FortiGuard Antispam service. | 53 |
| ddns-server-ip <IPv4_addr> | Enter the IP address of the FortiDDNS service. | 0.0.0.0 |
| ddns-server-port <port_int> | Enter the port used for FortiDDNS service. | 443 |
| service-account-id <id_str> | Enter the Service Account ID to use with communications with FortiGuard Analysis Service or FortiGuard Management Service. | No default. |
| service-account-passwd <pwd_str> | Enter the Service Account password to use for FortiGuard Analysis Service or FortiGuard Management Service. | No default. |
| load-balance-servers <number> | Enter the number of FortiGuard servers to connect to. By default, the FortiGate unit always uses the first server in its FortiGuard server list to connect to the FortiGuard network and <code>load-balance-servers</code> is set to 1. You can increase this number up to 20 if you want the FortiGate unit to use a different FortiGuard server each time it contacts the FortiGuard network. If you set <code>load-balance-servers</code> to 2, the FortiGate unit alternates between checking the first two servers in the FortiGuard server list. | 1 |
| antispam-cache {enable disable} | Enable or disable caching of FortiGuard Antispam query results, including IP address and URL block list. Enabling the cache can improve performance because the FortiGate unit does not need to access the FDN or FortiManager unit each time the same IP address or URL appears as the source of an email. When the cache is full, the least recently used cache entry is replaced. | enable |
| antispam-cache-ttl <tll_int> | Enter a time to live (TTL), in seconds, for antispam cache entries. When the TTL expires, the cache entry is removed, requiring the FortiGate unit to query the FDN or FortiManager unit the next time that item occurs in scanned traffic. Valid TTL ranges from 300 to 86400 seconds. | 1800 |
| antispam-cache-mpersent <ram_int> | Enter the maximum percentage of memory (RAM) to use for antispam caching. Valid percentage ranges from 1 to 15. | 2 |

| Variable | Description | Default |
|--|---|---------|
| antispam-expiration | The expiration date of the FortiGuard Antispam service contract. This variable can be viewed with the <code>get</code> command, but cannot be <code>set</code> . | N/A |
| antispam-force-off {enable disable} | Enable to stop FortiGuard Antispam service on this FortiGate unit. | disable |
| antispam-license | The interval of time between license checks for the FortiGuard Antispam service contract. This variable can be viewed with the <code>get</code> command, but cannot be <code>set</code> . | 7 |
| antispam-timeout <timeout_int> | Enter the FortiGuard Antispam query timeout. Valid timeout ranges from 1 to 30 seconds. | 7 |
| avquery-cache {enable disable} | Enable or disable caching of FortiGuard Antivirus query results. Enabling the cache can improve performance because the FortiGate unit does not need to access the FDN each time the same IP address or URL appears as the source of an email. When the cache is full, the least recently used cache entry is replaced. | enable |
| avquery-cache-ttl <ttl_int> | Enter a time to live (TTL), in seconds, for antivirus cache entries. When the TTL expires, the cache entry is removed, requiring the FortiGate unit to query the FDN or FortiManager unit the next time that item occurs in scanned traffic. Valid TTL ranges from 300 to 86400 seconds. | 1800 |
| avquery-cache-mpercent <max_int> | Enter the maximum memory to be used for FortiGuard Antivirus query caching. Valid percentage ranges from 1 to 15. | 2 |
| avquery-force-off {enable disable} | Enable to stop FortiGuard Antivirus service on this FortiGate unit. | disable |
| avquery-license | The interval of time between license checks for the FortiGuard Antivirus service contract. This variable can be viewed with the <code>get</code> command, but cannot be <code>set</code> . | Unknown |
| avquery-expiration | The expiration date of the FortiGuard Antivirus service contract. This variable can be viewed with the <code>get</code> command, but cannot be <code>set</code> . | N/A |
| avquery-timeout <timeout_int> | Enter the time limit in seconds for the FortiGuard Antivirus service query timeout. Valid timeout ranges from 1 to 30. | 7 |
| webfilter-cache {enable disable} | Enable or disable caching of FortiGuard Web Filtering query results, including category ratings for URLs. Enabling the cache can improve performance because the FortiGate unit does not need to access the FDN or FortiManager unit each time the same IP address or URL is requested. When the cache is full, the least recently used cache entry is replaced. | enable |

| Variable | Description | Default |
|---|---|---------|
| webfilter-cache-ttl <ttl_int> | Enter a time to live (TTL), in seconds, for web filtering cache entries. When the TTL expires, the cache entry is removed, requiring the FortiGate unit to query the FDN or FortiManager unit the next time that item occurs in scanned traffic. Valid TTL ranges from 300 to 86400 seconds. | 3600 |
| webfilter-expiration | The expiration date of the FortiGuard Web Filtering service contract. This variable can be viewed with the <code>get</code> command, but cannot be <code>set</code> . | N/A |
| webfilter-force-off {enable disable} | Enable to stop FortiGuard Webfilter service on this FortiGate unit. | disable |
| webfilter-license | The interval of time between license checks for the FortiGuard Web Filtering service contract. Initially, this value is unknown, and is set after contacting the FDN to validate the FortiGuard Web Filtering license. This variable can be viewed with the <code>get</code> command, but cannot be <code>set</code> . | Unknown |
| webfilter-sdns-server-ip | Enter the IP address of the FortiDNS server. This is used for DNS-based web filtering. | 0.0.0.0 |
| webfilter-sdns-server-port | Enter the TCP port of the FortiDNS server. This is used for DNS-based web filtering. | 443 |
| webfilter-timeout <timeout_int> | Enter the FortiGuard Web Filtering query timeout. Valid timeout ranges from 1 to 30 seconds. | 15 |

fortisandbox

Use this command to configure the FortiGate unit to use the FortiSandbox appliance.

Syntax

```
config system fortisandbox
  set status {enable | disable}
  set server <server_ip>
  set email <email_addr>
  set source-ip <ip_addr>
  set enc-algorithm {enable | disable}
end
```

| Variable | Description | Default |
|----------------------------------|---|-------------|
| status {enable disable} | Enable use of FortiSandbox. | |
| server <server_ip> | Enter the FortiSandbox server IP address. | No default. |
| email <email_addr> | Enter the notifier email address. | No default. |
| source-ip <ip_addr> | Enter the source IP address to use for communication to FortiSandbox. | |
| enc-algorithm {enable disable} | Enable or disable use of SSL encryption for FortiSandbox data. | |

geoip-override

Use this command to override geolocation mappings that are not correct in the FortiGate init's database.

Syntax

```
config system geoip-override
  edit <name_str>
    set description <desc_str>
    config ip-range
      edit <range_id>
        set start-ip <IPv4_addr>
        set end-ip <IPv4_addr>
      end
    end
  end
```

| Variable | Description | Default |
|---------------------------|--|-------------|
| <name_str> | Enter a name for this geolocation override. | No default. |
| description <desc_str> | Enter a description for this geolocation override. Maximum length 128 characters. | No default. |
| <range_id> | Enter a integer ID for this range entry. | No default. |
| start-ip <IPv4_addr> | Enter the first IP address of the range. | No default. |
| end-ip <IPv4_addr> | Enter the last IP address of the range. | No default. |

gi-gk

This command configures the settings for the FortiOS Carrier Gi gateway firewall. This firewall is used in the anti-overbilling configuration, and can be enabled on a per interface basis. For more information see [“system interface” on page 555](#).

Syntax

```
config system gi-gk
  set context <id_integer>
  set port <tcp_port>
end
```

| Variable | Description | Default |
|----------------------|--|---------|
| context <id_integer> | Enter the context ID for the Gi gateway firewall | |
| port <tcp_port> | Enter the TCP port to listen to. Valid range is from 0 to 65535. | 0 |

global

Use this command to configure global settings that affect various FortiGate systems and configurations.

Runtime-only config mode was introduced in FortiOS v3.0 MR2. This mode allows you to try out commands that may put your FortiGate unit into an unrecoverable state normally requiring a physical reboot. In runtime-only config mode you can set a timeout so after a period of no input activity the FortiGate unit will reboot with the last saved configuration. Another option in runtime-only configuration mode is to manually save your configuration periodically to preserve your changes. For more information see `set cfg-save {automatic | manual | revert}`, `set cfg-revert-timeout <seconds>`, and execute `cfg reload`.

Syntax

```
config system global
    set admin-concurrent {enable | disable}
    set admin-console-timeout <secs_int>
    set admin-https-pki-required {enable | disable}
    set admin-https-redirect {enable | disable}
    set admin-lockout-duration <time_int>
    set admin-lockout-threshold <failed_int>
    set admin-maintainer {enable | disable}
    set admin-port <port_number>
    set admin-reset-button {enable | disable}
    set admin-scp {enable | disable}
    set admin-server-cert { self-sign | <certificate> }
    set admin-sport <port_number>
    set admin-ssh-grace-time <time_int>
    set admin-ssh-port <port_number>
    set admin-ssh-v1 {enable | disable}
    set admin-telnet-port <port_number>
    set admintimeout <admin_timeout_minutes>
    set allow-traffic-redirect {enable | disable}
    set anti-replay {disable | loose | strict}
    set auth-cert <cert-name>
    set auth-http-port <http_port>
    set auth-https-port <https_port>
    set auth-keepalive {enable | disable}
    set auth-policy-exact-match {enable | disable}
    set av-failopen {idledrop | off | one-shot | pass}
    set av-failopen-session {enable | disable}
    set batch-cmdb {enable | disable}
    set block-session-timer <int>
    set cert-chain-max <int>
    set cfg-save {automatic | manual | revert}
    set cfg-revert-timeout <seconds>
    set check-protocol-header {loose | strict}
    set check-reset-range {disable | strict}
    set clt-cert-req {enable | disable}
```

```
set csr-ca-attribute {enable | disable}
set daily-restart {enable | disable}
set detection-summary {enable | disable}
set dst {enable | disable}
set elbc-status {enable | disable}
set endpoint-control-fds-access {enable | disable}
set endpoint-control-portal-port <endpoint_port>
set explicit-proxy-auth-timeout <seconds_int>
set fds-statistics {enable | disable}
set fds-statistics-period <minutes>
set fgd-alert-subscription {advisory latest-threat latest-virus
    latest-attack new-virus-db new-attack-db}
set fmc-xg2-load-balance {disable | enable}
set forticlient-reg-port <int>
set fwpolicy-implicit log {enable | disable}
set fwpolicy6-implicit log {enable | disable}
set gui-antivirus {enable | disable}
set gui-application-control {enable | disable}
set gui-ap-profile {disable | enable}
set gui-central-nat-table {disable | enable}
set gui-certificates {enable | disable}
set gui-client-reputation {enable | disable}
set gui-dlp {enable | disable}
set gui-dns-database {disable | enable}
set gui-dynamic-profile-display {disable | enable}
set gui-dynamic-routing {enable | disable}
set gui-endpoint-control {enable | disable}
set gui-explicit-proxy {enable | disable}
set gui-icap {disable | enable}
set gui-implicit-policy {disable | enable}
set gui-ips {enable | disable}
set gui-ipsec-manual-key {enable | disable}
set gui-ipv6 {enable | disable}
set gui-lines-per-page <gui_lines>
set gui-load-balance {disable | enable}
set gui-multicast-policy {enable | disable}
set gui-multiple-utm-profiles {enable | disable}
set gui-nat46-64 {enable | disable}
set gui-object-tags {enable | disable}
set gui-policy-based-ipsec {enable | disable}
set gui-replacement-message-groups {enable | disable}
set gui-spamfilter {enable | disable}
set gui-sslvpn-personal-bookmarks {enable | disable}
set gui-sslvpn-realms {enable | disable}
set gui-voip-profile {disable | enable}
set gui-vpn {enable | disable}
set gui-vulnerability-scan {enable | disable}
set gui-wanopt-cache {enable | disable}
set gui-webfilter {enable | disable}
```

```
set gui-wireless-controller {enable | disable}
set gui-wireless-opensecurity {enable | disable}
set hostname <unithostname>
set http-obfuscate {header-only | modified | no-error | none}
set ie6workaround {enable | disable}
set internal-switch-mode {hub | interface | switch}
set internal-switch-speed {100full | 100half | 10full | 10half
    | auto}
set ip-src-port-range <start_port>-<end_port>
set ipsec-hmac-offload {disable | enable}
set ipv6-accept-dad {0|1|2}
set language <language>
set lcdpin <pin_number>
set lcdprotection {enable | disable}
set ldapconntimeout <ldaptimeout_msec>
set login-timestamp {enable | disable}
set log-user-in-upper {enable | disable}
set management-vdom <domain>
set max-dlpstat-memory <size>
set max-report-db-size <size>
set miglogd-children <int>
set num-cpus <int>
set optimize {antivirus | throughput}
set optimize-ssl {enable | disable}
set phase1-rekey {enable | disable}
set policy-auth-concurrent <limit_int>
set per-user-bwl {enable | disable}
set pre-login-banner {enable | disable}
set proxy-worker-count <count_int>
set post-login-banner {enable | disable}
set radius-port <radius_port>
set refresh <refresh_seconds>
set registration-notification {disable | enable}
set remoteauthtimeout <timeout_sec>
set reset-sessionless-tcp {enable | disable}
set restart-time <hh:mm>
set revision-backup-on-logout {enable | disable}
set revision-image-auto-backup {enable | disable}
set scanunit-count <count_int>
set send-pmtu-icmp {enable | disable}
set service-expire-notification {disable | enable}
set show-backplane-intf {enable | disable}
set sql-logging {enable | disable}
set sp-load-balance {enable | disable}
set sslvpn-cipher-hardware-acceleration {enable | disable}
set sslvpn-kxp-hardware-acceleration {enable | disable}
set sslvpn-pkce2-hardware-acceleration {enable | disable}
set sslvpn-max-worker-count <count_int>
set sslvpn-personal-bookmark-mgmt {enable | disable}
```

```

set sslvpn-worker-count <count_int>
set strict-dirty-session-check {enable | disable}
set strong-crypto {enable | disable}
set switch-controller {enable | disable}
set switch-controller-reserved-network <ipv4mask>
set tcp-halfclose-timer <seconds>
set tcp-halfopen-timer <seconds>
set tcp-option {enable | disable}
set tcp-timewait-timer <seconds_int>
set timezone <timezone_number>
set tos-based-priority {low | medium | high}
set tp-mc-skip-policy {enable | disable}
set two-factor-email-expiry <seconds_int>
set two-factor-ftm-expiry <hours_int>
set two-factor-sms-expiry <seconds_int>
set udp-idle-timer <seconds>
set usb-wan-auth-type {none | pap | chap}
set usb-wan-extra-init <init_str>
set usb-wan-passwd <str>
set usb-wan-username <str>
set use-usb-wan {enable | disable}
set user-server-cert <cert_name>
set vdom-admin {enable | disable}
set vip-arp-range {unlimited | restricted}
set virtual-server-count <integer>
set virtual-server-hardware-acceleration {enable | disable}
set wan {enable | disable}
set wifi-certificate <cert-name>
set wifi-ca-certificate <ca_cert-name>
set wimax-4g-usb {enable | disable}
set wireless-controller {enable | disable}
set wireless-controller-port <port_int>
set wireless-mode {ac | client}
end

```

| Variable | Description | Default |
|--|---|---------|
| admin-concurrent {enable disable} | Enable to allow concurrent administrator logins. When disabled, the FortiGate unit restricts concurrent access from the same admin user name but on a different IP address. Use policy-auth-concurrent for firewall authenticated users. | enable |
| admin-console-timeout <secs_int> | Set a console login timeout that overrides the admintimeout value. Range 15 to 300 seconds. A zero value disables this timeout. | 0 |
| admin-https-pki-required {enable disable} | Enable to allow user to login by providing a valid certificate if PKI is enabled for HTTPS administrative access. Default setting disable allows admin users to log in by providing a valid certificate or password. | disable |

| Variable | Description | Default |
|--|--|-----------|
| admin-https-redirect { enable disable } | Enable redirection of HTTP administration access to HTTPS. This is not available on low-crypto units. | disable |
| admin-lockout-duration <time_int> | Set the administration account's lockout duration in seconds for the firewall. Repeated failed login attempts will enable the lockout. Use admin-lockout-threshold to set the number of failed attempts that will trigger the lockout. | 60 |
| admin-lockout-threshold <failed_int> | Set the threshold, or number of failed attempts, before the account is locked out for the admin-lockout-duration. | 3 |
| admin-maintainer { enable disable } | Enables or disables the special hidden "maintainer" user login, which is used for password recovery. When enabled, the "maintainer" account can log in from the console after a hard reboot (power off, power on) using the password "bcpb" followed by the FortiGate unit serial number. You have limited time to complete this login. | enable |
| admin-port <port_number> | Enter the port to use for HTTP administrative access. | 80 |
| admin-reset-button { enable disable } | Enable or disable use of FortiGate unit reset button. Even if enabled, the button is active for only 30 seconds after boot-up. | enable |
| admin-scp { enable disable } | Enable to allow system configuration download by the secure copy (SCP) protocol. | disable |
| admin-server-cert { self-sign <certificate> } | Select the admin https server certificate to use. Choices include self-sign, and the filename of any installed certificates. | self-sign |
| admin-sport <port_number> | Enter the port to use for HTTPS administrative access. | 443 |
| admin-ssh-grace-time <time_int> | Enter the maximum time permitted between making an SSH connection to the FortiGate unit and authenticating. Range is 10 to 3600 seconds. | 120 |
| admin-ssh-port <port_number> | Enter the port to use for SSH administrative access. | 22 |
| admin-ssh-v1 { enable disable } | Enable compatibility with SSH v1.0. | disable |
| admin-telnet-port <port_number> | Enter the port to use for telnet administrative access. | 23 |
| admintimeout <admin_timeout_minutes> | Set the number of minutes before an idle administrator times out. This controls the amount of inactive time before the administrator must log in again. The maximum admintimeout interval is 480 minutes (8 hours). To improve security keep the idle timeout at the default value of 5 minutes. | 5 |
| allow-traffic-redirect { enable disable } | Under some conditions, it is undesirable to have traffic routed back on the same interface. In that case, set allow-traffic-redirect to disable. | enable |

| Variable | Description | Default |
|--|--|-----------|
| anti-replay {disable loose strict} | <p>Set the level of checking for packet replay and TCP sequence checking (or TCP Sequence (SYN) number checking). All TCP packets contain a Sequence Number (SYN) and an Acknowledgement Number (ACK). The TCP protocol uses these numbers for error free end-to-end communications. TCP sequence checking can also be used to validate individual packets.</p> <p>FortiGate units use TCP sequence checking to make sure that a packet is part of a TCP session. By default, if a packet is received with sequence numbers that fall out of the expected range, the FortiGate unit drops the packet. This is normally a desired behavior, since it means that the packet is invalid. But in some cases you may want to configure different levels of anti-replay checking if some of your network equipment uses non-RFC methods when sending packets. You can set anti-replay protection to the following settings:</p> <p>disable No anti-replay protection.</p> <p>loose Perform packet sequence checking and ICMP anti-replay checking with the following criteria:</p> <ul style="list-style-type: none"> • The SYN, FIN, and RST bit can not appear in the same packet. • The FortiGate unit does not allow more than 1 ICMP error packet to go through the FortiGate unit before it receives a normal TCP or UDP packet. • If the FortiGate unit receives an RST packet, and <code>check-reset-range</code> is set to <code>strict</code> the FortiGate unit checks to determine if its sequence number in the RST is within the un-ACKed data and drops the packet if the sequence number is incorrect. <p>strict Performs all of the loose checking but for each new session also checks to determine if the TCP sequence number in a SYN packet has been calculated correctly and started from the correct value for each new session. Strict anti-replay checking can also help prevent SYN flooding.</p> <p>If any packet fails a check it is dropped. If “log-invalid-packet {enable disable}” on page 298 is enabled a log message is written for each packet that fails a check.</p> | strict |
| auth-cert <cert-name> | <p>HTTPS server certificate for policy authentication.</p> <p>Self-sign is the built in certificate but others will be listed as you add them.</p> | self-sign |
| auth-http-port <http_port> | Set the HTTP authentication port. <http_port> can be from 1 to 65535. | 1000 |

| Variable | Description | Default |
|---|---|---------|
| auth-https-port <https_port> | Set the HTTPS authentication port. <https_port> can be from 1 to 65535. | 1003 |
| auth-keepalive {enable disable} | Enable to extend the authentication time of the session through periodic traffic to prevent an idle timeout. | disable |
| auth-policy-exact-match {enable disable} | Enable to require traffic to exactly match an authenticated policy with a policy id and IP address to pass through. When disabled, only the IP needs to match. | disable |
| av-failopen {idledrop off one-shot pass} | <p>Set the action to take if the unit is running low on memory or the proxy connection limit has been reached. Valid options are <code>idledrop</code>, <code>off</code>, <code>one-shot</code>, and <code>pass</code>.</p> <ul style="list-style-type: none"> <code>idledrop</code> – drop connections based on the clients that have the most connections open. This is most useful for Windows applications, and can prevent malicious bots from keeping an idle connection open to a remote server. <code>off</code> – stop accepting new AV sessions when entering conserve mode, but continue to process current active sessions. <code>one-shot</code> – bypass the antivirus system when memory is low. You must enter <code>off</code> or <code>pass</code> to restart antivirus scanning. <code>pass</code> – bypass the antivirus system when memory is low. Antivirus scanning resumes when the low memory condition is resolved. | pass |
| av-failopen-session {enable disable} | When enabled and a proxy for a protocol runs out of room in its session table, that protocol goes into failopen mode and enacts the action specified by <code>av-failopen</code> . | disable |
| batch-cmdb {enable disable} | <p>Enable/disable batch mode.</p> <p>Batch mode is used to enter a series of commands, and executing the commands as a group once they are loaded. For more information, see “execute batch” on page 910.</p> | enable |
| block-session-timer <int> | Enter the time duration for blocked sessions. Range: 1 to 300 seconds. | 30 |
| cert-chain-max <int> | Set maximum depth for a certificate chain. | 8 |

| Variable | Description | Default |
|--|---|-----------|
| cfg-save {automatic manual revert} | <p>Set the method for saving the FortiGate system configuration and enter into runtime-only configuration mode. Methods for saving the configuration are:</p> <ul style="list-style-type: none"> <code>automatic</code> – automatically save the configuration after every change. <code>manual</code> – manually save the configuration using the execute cfg save command. <code>revert</code> – manually save the current configuration and then revert to that saved configuration after <code>cfg-revert-timeout</code> expires. <p>Switching to automatic mode disconnects your session.</p> <p>This command is used as part of the runtime-only configuration mode.</p> <p>See “execute cfg reload” on page 914 for more information.</p> | automatic |
| cfg-revert-timeout <seconds> | <p>Enter the timeout interval in seconds. If the administrator makes a change and there is no activity for the timeout period, the FortiGate unit will automatically revert to the last saved configuration. Default timeout is 600 seconds.</p> <p>This command is available only when <code>cfg-save</code> is set to <code>revert</code>.</p> <p>This command is part of the runtime-only configuration mode. See “execute cfg reload” on page 914 for more information.</p> | 600 |
| check-protocol-header {loose strict} | <p>Select the level of checking performed on protocol headers.</p> <ul style="list-style-type: none"> <code>loose</code> – the FortiGate unit performs basic header checking to verify that a packet is part of a session and should be processed. Basic header checking includes verifying that the layer-4 protocol header length, the IP header length, the IP version, the IP checksum, IP options are correct, etc. <code>strict</code> – the FortiGate unit does the same checking as above plus it verifies that ESP packets have the correct sequence number, SPI, and data length. <p>If the packet fails header checking it is dropped by the FortiGate unit and logged if “log-invalid-packet {enable disable}” on page 298 is enabled.</p> | loose |

| Variable | Description | Default |
|--|--|---------|
| check-reset-range {disable strict} | Configure ICMP error message verification. <ul style="list-style-type: none"> <code>disable</code> – the FortiGate unit does not validate ICMP error messages. <code>strict</code> – If the FortiGate unit receives an ICMP error packet that contains an embedded IP(A,B) TCP(C,D) header, then if FortiOS can locate the A:C->B:D session it checks to make sure that the sequence number in the TCP header is within the range recorded in the session. If the sequence number is not in range then the ICMP packet is dropped. If “log-invalid-packet {enable disable}” on page 298 is enabled the FortiGate unit logs that the ICMP packet was dropped. Strict checking also affects how the <code>anti-replay</code> option checks packets. | disable |
| clt-cert-req {enable disable} | Enable to require a client certificate before an administrator logs on to the web-based manager using HTTPS. | disable |
| csr-ca-attribute {enable disable} | Enable to use the CA attribute in your certificate. Some CA servers reject CSRs that have the CA attribute. | enable |
| daily-restart {enable disable} | Enable to restart the FortiGate unit every day. The time of the restart is controlled by <code>restart-time</code> . | disable |
| detection-summary {enable disable} | Disable to prohibit the collection of detection summary statistics for FortiGuard. | enable |
| dst {enable disable} | Enable or disable daylight saving time. If you enable daylight saving time, the FortiGate unit adjusts the system time when the time zone changes to daylight saving time and back to standard time. | enable |
| elbc-status {enable disable} | This attribute is enabled by default. When enabled the system will await the base channel heartbeat that will configure the system into ELBCv3 mode. Disabling this command will not disable ELBCv3 mode once the FortiGate has already configured itself for ELBCv3 mode. See “system elbc” on page 513 . | enable |
| endpoint-control-fds-access {enable disable} | Enable or disable access to FortiGuard servers for non-compliant endpoints. | enable |
| endpoint-control-portal-port <endpoint_port> | Enter the port number from 1 to 65535 for the endpoint control portal port for FortiClient downloads. | 8009 |
| explicit-proxy-auth-timeout <seconds_int> | Enter the timeout, in seconds, for idle explicit web proxy sessions. Range: 1 to 600 seconds. | 300 |
| fds-statistics {enable disable} | Enable or disable AV/IPS signature reporting. If necessary, disable to avoid error messages on HA subordinate units during an AV/IPS update. | enable |

| Variable | Description | Default |
|---|---|---|
| fds-statistics-period <minutes> | Select the number of minutes in the FDS report period. Range is 1 to 1440 minutes. | 60 |
| fgd-alert-subscription { advisory latest-threat latest-virus latest-attack new-virus-db new-attack-db } | Select what to retrieve from FortiGuard: advisory — FortiGuard advisories, report and news alerts latest-attack — latest FortiGuard attack alerts latest-threat — latest FortiGuard threats alerts latest-virus — latest FortiGuard virus alerts new-antivirus-db — FortiGuard AV database release alerts new-attack-db — FortiGuard IPS database release alerts. | null |
| fmc-xg2-load-balance { disable enable } | Enable to start XG2 load balancing. | disable |
| forticlient-reg-port <int> | Change the FortiClient registration port. This might be necessary if the default port is used for some other purpose. The registration IP address is the IP address of the interface whose listen-for-forticlient-registration is enabled. | 8010 |
| fwpolicy-implicit log { enable disable } | Enable to log when a session uses an implicit policy (IPv4). | disable |
| fwpolicy6-implicit log { enable disable } | Enable to log when a session uses an implicit policy (IPv6). | disable |
| gui-antivirus { enable disable } | Enable or disable antivirus profiles in the web-based manager. | enable |
| gui-application-control { enable disable } | Enable or disable application control options in the web-based manager. | enable |
| gui-ap-profile { disable enable } | Enable or disable custom AP profile configuration options on the web-based manager. | enable, except disable on model 30D |
| gui-central-nat-table { disable enable } | Enable or disable central NAT table configuration options and display on the web-based manager. | disable |
| gui-certificates { enable disable } | Enable or disable display of certificate configuration in the web-based manager. | Enabled on rack-mount units. |
| gui-client-reputation { enable disable } | Enable or disable display of client reputation configuration in the web-based manager. | enable |
| gui-dlp { enable disable } | Enables Data Leak Prevention in the web-based manager. | Depends on model. |
| gui-dns-database { disable enable } | Enable to display the DNS database menu in the web-based manager interface. | disable |
| gui-dynamic-profile- display { disable enable } | Enable to display dynamic profile feature controls in the web-based manager. | enable |

| Variable | Description | Default |
|---|---|------------------------------|
| gui-dynamic-routing {enable disable} | Enable dynamic routing in the web-based manager. If disabled, the Routing menu is removed. Static routing is available in <i>System > Network > Routing</i> and route monitoring in <i>System > Monitor > Routing Monitor</i> . | Depends on model. |
| gui-endpoint-control {enable disable} | Enable to display the endpoint control feature in the web-based manager. | enable |
| gui-explicit-proxy {enable disable} | Enable or disable display of Explicit Proxy configuration options on the web-based manager. | Enabled on rack-mount units. |
| gui-icap {disable enable} | Enable or disable ICAP configuration options on the web-based manager. | disable |
| gui-implicit-policy {disable enable} | Enable or disable implicit firewall policy configuration options on the web-based manager. | enable |
| gui-ips {enable disable} | Enable or disable display of the IPS sensors in the web-based manager | enable |
| gui-ipsec-manual-key {enable disable} | Enable to display the IPsec manual key page on the web-based manager. | disable |
| gui-ipv6 {enable disable} | Enable or disable IPv6 configuration options on the web-based manager. | disable |
| gui-lines-per-page <gui_lines> | Set the number of lines displayed on table lists. Range is from 20 - 1000 lines per page. | 50 |
| gui-load-balance {disable enable} | Enable or disable display of Load Balance in web-based manager Firewall Objects menu. | disable |
| gui-multicast-policy {enable disable} | Enables or disables display of multicast firewall policies in the web-based manager. | disable |
| gui-multiple-utm-profiles {enable disable} | Enables or disables display of multiple UTM profiles in the web-based manager. | enable |
| gui-nat46-64 {enable disable} | Enables or disables display of NAT46 and NAT64 settings in the web-based manager. | disable |
| gui-object-tags {enable disable} | Enable or disable object tagging and object coloring configuration options on the web-based manager. | disable |
| gui-policy-based-ipsec {enable disable} | Enable or disable display of policy-based IPsec VPN options in the web-based manager. | disable |
| gui-replacement-message-groups {enable disable} | Enable or disable display of Replacement Message Groups feature in the web-based manager. | Enabled on rack-mount units. |
| gui-spamfilter {enable disable} | Enable or disable display of spamfilter profiles in the web-based manager. | enable |
| gui-sslvpn-personal-bookmarks {enable disable} | Enable personal SSL VPN bookmark management in the SSLVPN portal. | Depends on model. |
| gui-sslvpn-realms {enable disable} | Enable SSL VPN realms in the web-based manager. | disable |
| gui-voip-profile {disable enable} | Enable or disable VoIP profile configuration options on the web-based manager. | disable |
| gui-vpn {enable disable} | Enable or disable VPN tunnel configuration in the web-based manager. | enable |

| Variable | Description | Default |
|--|---|-------------------------------------|
| gui-vulnerability-scan { enable disable } | Enable or disable display of the vulnerability scan in the web-based manager. | enable |
| gui-wanopt-cache { enable disable } | Enable or disable display of WAN Optimization configuration options on the web-based manager. | Enabled on rack-mount units. |
| gui-webfilter { enable disable } | Enable or disable display of webfilter profiles in the web-based manager | enable |
| gui-wireless-controller { enable disable } | Enable or disable display of the wireless controller configuration in the web-based manager. | enable, except disable on model 30D |
| gui-wireless-opensecurity { enable disable } | Enable or disable display of open security option for SSID in the web-based manager. | disable |
| hostname <unithostname> | <p>Enter a name to identify this FortiGate unit. A hostname can only include letters, numbers, hyphens, and underlines. No spaces are allowed.</p> <p>While the hostname can be longer than 16 characters, if it is longer than 16 characters it will be truncated and end with a “~” to indicate it has been truncated. This shortened hostname will be displayed in the CLI, and other locations the hostname is used.</p> <p>Some models support hostnames up to 35 characters.</p> <p>By default the hostname of your FortiGate unit is its serial number which includes the model.</p> | FortiGate serial number. |
| http-obfuscate { header-only modified no-error none } | <p>Set the level at which the identity of the FortiGate web server is hidden or obfuscated in the browser address field, including URLs provided via SSL VPN Bookmarks (web mode only).</p> <p>none — do not hide the FortiGate web server identity.</p> <p>header-only — hides the HTTP server banner.</p> <p>modified — provides modified error responses.</p> <p>no-error — suppresses error responses.</p> | none |
| ie6workaround { enable disable } | Enable or disable the work around for a navigation bar freeze issue caused by using the FortiGate web-based manager with Internet Explorer 6. | disable |

| Variable | Description | Default |
|--|--|-----------|
| internal-switch-mode {hub interface switch} | <p>Set the mode for the internal switch to be one of hub, interface, or switch.</p> <p>Switch mode combines FortiGate unit interfaces into one switch with one address. Interface mode gives each internal interface its own address.</p> <p>On some FortiGate models you can also select <i>Hub Mode</i>. Hub mode is similar to switch mode except that in hub mode the interfaces do not learn the MAC addresses of the devices on the network they are connected to and may also respond quicker to network changes in some circumstances. You should only select <i>Hub Mode</i> if you are having network performance issues when operating with switch mode. The configuration of the FortiGate unit is the same whether in switch mode or hub mode.</p> <p>Before switching modes, all configuration settings for the interfaces affected by the switch must be set to defaults.</p> | switch |
| internal-switch-speed {100full 100half 10full 10half auto} | <p>Set the speed of the switch used for the internal interface. Choose one of:</p> <p>100full</p> <p>100half</p> <p>10full</p> <p>10half</p> <p>auto</p> <p>100 and 10 refer to 100M or 10M bandwidth. Full and half refer to full or half duplex.</p> | auto |
| ip-src-port-range <start_port>-<end_port> | <p>Specify the IP source port range used for traffic originating from the FortiGate unit. The valid range for <start_port> and <end_port> is from 1 to 65535 inclusive.</p> <p>You can use this setting to avoid problems with networks that block some ports, such as FDN ports.</p> | 1024-4999 |
| ipsec-hmac-offload {disable enable} | Enable to offload IPsec HMAC processing to hardware or disable to perform IPsec HMAC processing in software. | enable |
| ipv6-accept-dad {0 1 2} | <p>Configure ipv6 DAD (Duplicate Address Detection) operation:</p> <p>0 — Disable DAD</p> <p>1 — Enable DAD</p> <p>2 — Enable DAD and disable IPv6 operation if MAC-based duplicate link-local address has been found.</p> | 1 |
| language <language> | Set the web-based manager display language. You can set <language> to one of english, french, japanese, korean, portuguese, spanish, simch (Simplified Chinese) or trach (Traditional Chinese). | english |

| Variable | Description | Default |
|---|--|-----------|
| lcdpin <pin_number> | Set the 6 digit PIN administrators must enter to use the LCD panel. This applies only to models with an LCD panel. | 123456 |
| lcdprotection {enable disable} | Enable or disable LCD panel PIN protection. This applies only to models with an LCD panel. | disable |
| ldapconntimeout <ldaptimeout_msec> | LDAP connection timeout in msec | 500 |
| login-timestamp {enable disable} | Enable or disable logging of login timestamps. | disable |
| log-user-in-upper {enable disable} | Log username in uppercase letters. | disable |
| management-vdom <domain> | Enter the name of the management virtual domain. Management traffic such as FortiGuard traffic originates from the management VDOM. | root |
| max-dlpstat-memory <size> | Enter the memory limit (1 to 15% of system memory) for the DLP stat daemon. | 5 |
| max-report-db-size <size> | Set the maximum size in MBytes for the log report database. | 1024 |
| miglogd-children <int> | Set the number of miglogd process to run. Range 0 to 15. | 0 |
| num-cpus <int> | Enter the number of active CPUs. | |
| optimize {antivirus throughput} | NOTE: Do <i>not</i> use this command. It is obsolete and can affect performance. The command will be removed in a later firmware release. The command was originally added to some early NP4 platforms but is no longer supported. | antivirus |
| optimize-ssl {enable disable} | Enable optimization of SSL by using multiple processes. | disable |
| optimize { | | antivirus |
| phase1-rekey {enable disable} | Enable or disable automatic rekeying between IKE peers before the phase 1 keylife expires. | enable |
| policy-auth-concurrent <limit_int> | Limit the number of concurrent logins from the same user. Range 1 to 100. 0 means no limit. For admin accounts use <code>admin-concurrent</code> . | 0 |
| per-user-bwl {enable disable} | Enable or disable the webfilter per-user black/white list feature. | disable |
| pre-login-banner {enable disable} | Enable to display the admin access disclaimer message prior to login. For more information see “system replacemsg admin” on page 610 . | disable |
| proxy-worker-count <count_int> | Set the number of proxy worker processes. Range 1 to 8. | 4 |
| post-login-banner {enable disable} | Enable to display the admin access disclaimer message after successful login. | disable |
| radius-port <radius_port> | Change the default RADIUS port. The default port for RADIUS traffic is 1812. If your RADIUS server is using port 1645 you can use the CLI to change the default RADIUS port on your FortiGate unit. | 1812 |

| Variable | Description | Default |
|--|---|-------------|
| refresh <refresh_seconds> | Set the Automatic Refresh Interval, in seconds, for the web-based manager System Status Monitor. Enter 0 for no automatic refresh. | 0 |
| registration-notification {disable enable} | Enable or disable displaying the registration notification on the web-based manager if the FortiGate unit is not registered. | enable |
| remoteauthtimeout <timeout_sec> | The number of seconds that the FortiGate unit waits for responses from remote RADIUS, LDAP, or TACACS+ authentication servers. The range is 0 to 300 seconds, 0 means no timeout. To improve security keep the remote authentication timeout at the default value of 5 seconds. However, if a RADIUS request needs to traverse multiple hops or several RADIUS requests are made, the default timeout of 5 seconds may not be long enough to receive a response. | 5 |
| reset-sessionless-tcp {enable disable} | Enabling this option may help resolve issues with a problematic server, but it can make the FortiGate unit more vulnerable to denial of service attacks. In most cases you should leave <code>reset-sessionless-tcp</code> disabled. The <code>reset-sessionless-tcp</code> command determines what action the FortiGate unit performs if it receives a TCP packet but cannot find a corresponding session in its session table. This happens most often because the session has timed out. If you disable <code>reset-sessionless-tcp</code> , the FortiGate unit silently drops the packet. The packet originator does not know that the session has expired and might re-transmit the packet several times before attempting to start a new session. This is normal network operation. If you enable <code>reset-sessionless-tcp</code> , the FortiGate unit sends a RESET packet to the packet originator. The packet originator ends the current session, but it can try to establish a new session. This is available in NAT/Route mode only. | disable |
| restart-time <hh:mm> | Enter daily restart time in hh:mm format (hours and minutes). This is available only when <code>daily-restart</code> is enabled. | No default. |
| revision-backup-on-logout {enable disable} | Enable or disable back up of the latest configuration revision when the administrator logs out of the CLI or web-based manager. | disable |
| revision-image-auto-backup {enable disable} | Enable or disable back up of the latest configuration revision when firmware is upgraded. | disable |

| Variable | Description | Default |
|---|---|------------------------------|
| scanunit-count <count_int> | Tune the number of scanunits. The range and default depend on the number of CPUs. Only available on FortiGate units with multiple CPUs. Recommended for advanced users. | Depends on model. |
| send-pmtu-icmp {enable disable} | Select enable to send a path maximum transmission unit (PMTU) - ICMP destination unreachable packet. Enable if you need to support PTMUD protocol on your network to reduce fragmentation of packets. Disabling this command will likely result PMTUD packets being blocked by the unit. | enable |
| service-expire-notification {disable enable} | Enable or disable displaying a notification on the web-based manager 30 days before the FortiGate unit support contract expires. | enable |
| show-backplane-intf {enable disable} | Select enable to show FortiGate-5000 backplane interfaces as port9 and port10. Once these backplanes are visible they can be treated as regular physical interfaces. | disable |
| sql-logging {enable disable} | Enable for SQL logging. This option is present only on models that have hard disks rather than SSDs. Report generation on these models can be slow. | disable |
| sp-load-balance {enable disable} | Enable or disable SP load balancing on models 3950B, 3951B, or 3140B. Not available if <code>npu-cascade-cluster</code> is enabled in system npu . | disable |
| sslvpn-cipher-hardware-acceleration {enable disable} | Enable or disable SSLVPN hardware acceleration. | Depends on model. |
| sslvpn-kxp-hardware-acceleration {enable disable} | Enable or disable SSLVPN KXP hardware acceleration. | Depends on model. |
| sslvpn-pkce2-hardware-acceleration {enable disable} | Enable or disable SSLVPN PKCE2 hardware acceleration. | Depends on model. |
| sslvpn-max-worker-count <count_int> | Set the maximum number of SSL VPN processes. The actual maximum is the number of CPUs or this value, whichever is smaller. | Depends on number of CPUs |
| sslvpn-personal-bookmark-mgmt {enable disable} | Enable or disable management of SSLVPN user personal bookmarks in the web-based manager. | Enabled on rack-mount units. |
| sslvpn-worker-count <count_int> | Set the number of processes used to optimize SSL inspection. The actual maximum is the number of CPUs minus one or this value, whichever is smaller. | Depends on number of CPUs |
| strict-dirty-session-check {enable disable} | Enable to check the session against the original policy when revalidating. This can prevent dropping of redirected sessions when web-filtering and authentication are enabled together. If this option is enabled, the FortiGate unit deletes a session if a routing or policy change causes the session to no longer match the policy that originally allowed the session. | disable |

| Variable | Description | Default |
|---|---|--------------------------------|
| strong-crypto { enable disable } | <p>Enable to use strong encryption and only allow strong ciphers (AES, 3DES) and digest (SHA1) for HTTPS/SSH admin access.</p> <p>When strong encryption is enabled, HTTPS is supported by the following web browsers: Netscape 7.2, Netscape 8.0, Firefox, and Microsoft Internet Explorer 7.0 (beta).</p> <p>Note that Microsoft Internet Explorer 5.0 and 6.0 are not supported in strong encryption.</p> | disable |
| switch-controller { enable disable } | Enable switch controller feature. This is available on models that support the switch controller. | disable |
| switch-controller-reserved-network <ipv4mask> | Enable reserved network subnet for controlled switches. This is available when the switch controller is enabled. | 169.254.254.0 255.255.254.0 |
| syncinterval <ntpsync_minutes> | Enter how often, in minutes, the FortiGate unit should synchronize its time with the Network Time Protocol (NTP) server. The <code>syncinterval</code> number can be from 1 to 1440 minutes. Setting to 0 disables time synchronization. | 0 |
| tcp-halfclose-timer <seconds> | Enter how many seconds the FortiGate unit should wait to close a session after one peer has sent a FIN packet but the other has not responded. The valid range is from 1 to 86400 seconds. | 120 |
| tcp-halfopen-timer <seconds> | Enter how many seconds the FortiGate unit should wait to close a session after one peer has sent an open session packet but the other has not responded. The valid range is from 1 to 86400 seconds. | 10 |
| tcp-option { enable disable } | Enable SACK, timestamp and MSS TCP options. For normal operation <code>tcp-option</code> should be enabled. Disable for performance testing or in rare cases where it impairs performance. | enable |
| tcp-timewait-timer <seconds_int> | <p>Set the length of the TCP TIME-WAIT state in seconds. As described in RFC 793, the "TIME-WAIT state represents waiting for enough time to pass to be sure the remote TCP received the acknowledgment of its connection termination request".</p> <p>Reducing the time of the TIME-WAIT state means the FortiGate unit can close terminated sessions faster which means more new sessions can be opened before the session limit is reached.</p> <p>The valid range is 0 to 300 seconds. A value of 0 sets the TCP TIME-WAIT to 0 seconds</p> | 1 |
| timezone <timezone_number> | The number corresponding to your time zone from 00 to 72. Press ? to list time zones and their numbers. Choose the time zone for the FortiGate unit from the list and enter the correct number. | 00 |

| Variable | Description | Default |
|--|--|-----------------------------------|
| tos-based-priority {low medium high} | Select the default system-wide level of priority for Type of Service (TOS). TOS determines the priority of traffic for scheduling. Typically this is set on a per service type level. For more information, see “system tos-based-priority” on page 695 . The value of this field is the default setting for when TOS is not configured on a per service level. | high |
| tp-mc-skip-policy {enable disable} | Enable to allow skipping of the policy check, and to enable multicast through. | disable |
| two-factor-email-expiry <seconds_int> | Set the timeout period for email-based two-factor authentication. Range 30 to 300 seconds. | 60 |
| two-factor-ftm-expiry <hours_int> | Set the timeout period for FortiToken-based two-factor authentication. Range 1 to 168 hours. | 72 |
| two-factor-sms-expiry <seconds_int> | Set the timeout period for sms-based two-factor authentication. Range 30 to 300 seconds. | 60 |
| udp-idle-timer <seconds> | Enter the number of seconds before an idle UDP connection times out. The valid range is from 1 to 86400 seconds. | 180 |
| usb-wan-auth-type {none pap chap} | Select authentication protocol (PAP or CHAP) or no authentication. | none |
| usb-wan-extra-init <init_str> | Enter initialization string for modem (127 characters maximum). | null |
| usb-wan-passwd <str> | Enter the authentication password for PDP-IP calls. | null |
| usb-wan-username <str> | Enter the authentication username for PDP-IP calls. | null |
| use-usb-wan {enable disable} | Enable use of wireless 4G LTE USB modem on USB interface. | disable |
| user-server-cert <cert_name> | Select the certificate to use for https user authentication. Default setting is <code>Fortinet_Factory</code> , if available, otherwise <code>self-sign</code> . | See definition under Description. |
| vdom-admin {enable disable} | Enable to configure multiple virtual domains. | disable |
| vip-arp-range {unlimited restricted} | <code>vip-arp-range</code> controls the number of ARP packets the FortiGate unit sends for a VIP range. If <code>restricted</code> , the FortiGate unit sends ARP packets for only the first 8192 addresses in a VIP range. If <code>unlimited</code> , the FortiGate unit sends ARP packets for every address in the VIP range. | restricted |
| virtual-server-count <integer> | Enter the number of virtual server processes to create. The maximum is the number of CPU cores. This is not available on single-core CPUs. | 1 |
| virtual-server-hardware-acceleration {enable disable} | Enable or disable hardware acceleration. | enable |
| wan {enable disable} | On models FWF-20C-ADSL and FGT-20C-ADSL enables one of the switch port interfaces to act as a WAN port. | disable |

| Variable | Description | Default |
|---|---|-------------|
| wifi-certificate <cert-name> | Select the certificate to use for WiFi authentication. | No default. |
| wifi-ca-certificate <ca_cert-name> | Select the CA certificate that verifies the WiFi certificate. | No default. |
| wimax-4g-usb {enable disable} | Enable to allow access to a WIMAX 4G USB device. | disable |
| wireless-controller {enable disable} | Enable or disable the wireless (WiFi) daemon. | enable |
| wireless-controller-port <port_int> | Select the port used for the control channel in wireless controller mode (<i>wireless-mode</i> is <i>ac</i>). The range is 1024 through 49150. The data channel port is the control channel port number plus one. | 5246 |
| wireless-mode {ac client} | Set the wireless mode (for FortiWiFi units): <i>ac</i> —Wireless controller with local wireless <i>client</i> —Wireless client | ac |

gre-tunnel

Use this command to configure the tunnel for a GRE interface. A new interface of type “tunnel” with the same name is created automatically as the local end of the tunnel. This command is available only in NAT/Route mode.

To complete the configuration of a GRE tunnel, you need to:

- configure a firewall policy to pass traffic from the local private network to the tunnel interface
- configure a static route to the private network at the remote end of the tunnel using the GRE tunnel “device”
- optionally, define the IP addresses for each end of the tunnel to enable dynamic routing through the tunnel or to enable pinging of each end of the tunnel for testing

Syntax

```
config system gre-tunnel
  edit <tunnel_name>
    set interface <interface_name>
    set local-gw <localgw_IP>
    set remote-gw <remotegw_IP>
  end
```

| Variable | Description | Default |
|----------------------------|---|-------------|
| edit <tunnel_name> | Enter a name for the tunnel. | No default. |
| interface <interface_name> | Enter the physical, VLAN, or IPsec VPN interface that functions as the local end of the tunnel. | |
| local-gw <localgw_IP> | Enter the IP address of the local gateway. | |
| remote-gw <remotegw_IP> | Enter the IP address of the remote gateway. | |

ha

Use this command to enable and configure FortiGate high availability (HA) and virtual clustering.

You cannot enable HA mode if one of the FortiGate unit interfaces uses DHCP or PPPoE to acquire an IP address. If DHCP or PPPoE is configured, the `config ha mode` keyword is not available.

In HA mode, most settings are automatically synchronized among cluster units. The following settings are not synchronized:

- `override`
- `priority` (including the `secondary-vcluster priority`)
- `ha-mgt-interface-gateway`
- `cpu-threshold`, `memory-threshold`, `http-proxy-threshold`, `ftp-proxy-threshold`, `imap-proxy-threshold`, `nntp-proxy-threshold`, `pop3-proxy-threshold`, `smtp-proxy-threshold`
- The `ha-priority` setting of the `config router gwdetect` command
- The `config system interface` settings of the FortiGate interface that becomes an HA reserved management interface
- The `config system global hostname` setting

Syntax

```
config system ha
    set arps <arp_integer>
    set arps-interval <interval_integer>
    set authentication {enable | disable}
    set cpu-threshold <weight_int> <low_int> <high_int>
    set encryption {enable | disable}
    set ftp-proxy-threshold <weight_int> <low_int> <high_int>
    set gratuitous-arps {enable | disable}
    set group-id <id_integer>
    set group-name <name_str>
    set ha-eth-type <type_int>
    set ha-mgmt-status {enable | disable}
    set ha-mgmt-interface <interface_name>
    set ha-mgmt-interface-gateway <gateway_interface>
    set ha-uptime-diff-margin <diff_int>
    set hb-interval <interval_integer>
    set hb-lost-threshold <threshold_integer>
    set hbdev <interface_name> <priority_integer> [<interface_name>
        <priority_integer>]...
    set hc-eth-type <type_int>
    set helo-holddown <holddown_integer>
    set http-proxy-threshold <weight_int> <low_int> <high_int>
    set imap-proxy-threshold <weight_int> <low_int> <high_int>
    set l2ep-eth-type <type_int>
    set link-failed-signal {enable | disable}
    set load-balance-all {enable | disable}
    set load-balance-udp {enable | disable}
```

```
set memory-threshold <weight_int> <low_int> <high_int>
set minimum-worker-threshold <threshold_int>
set mode {a-a | a-p | standalone}
set monitor <interface_names>
set nntp-proxy-threshold <weight_int> <low_int> <high_int>
set override {enable | disable}
set password <password_str>
set pingserver-failover-threshold <threshold_integer>
set pingserver-flip-timeout <timeout_integer>
set pingserver-monitor-interface <interface_names>
set pop3-proxy-threshold <weight_int> <low_int> <high_int>
set priority <priority_integer>
set route-hold <hold_integer>
set route-ttl <ttl_integer>
set route-wait <wait_integer>
set schedule {hub | ip | ipport | leastconnection | none | random
              | round-robin | weight-round-robin}
set session-pickup {enable | disable}
set session-pickup-connectionless {enable | disable}
set session-pickup-delay {enable | disable}
set session-pickup-expectation {enable | disable}
set session-pickup-nat {enable | disable}
set session-sync-daemon-number <process_id_int>
set session-sync-dev <interface_name> [<interface_name>]...
set slave-switch-standby {enable | disable}
set smtp-proxy-threshold <weight_int> <low_int> <high_int>
set standalone-config-sync {enable | disable}
set sync-config {enable | disable}
set uninterruptible-upgrade {enable | disable}
set update-all-session-timer {enable | disable}
set weight <priority_integer> <weight_integer>
set vdom <vdom_names>
set vcluster2 {disable | enable}
end
config secondary-vcluster
    set monitor <interface_names>
    set override {enable | disable}
    set priority <priority_integer>
    set vdom <vdom_names>
    set pingserver-failover-threshold <threshold_integer>
    set pingserver-monitor-interface <interface_names>
end
config frup-settings
    set active-interface <interface_name>
    set backup-interface <interface_name>
    set active-switch-port <port_number>
end
end
```


| Variable | Description | Default |
|---|---|---------|
| arps <arp_integer> | Set the number of times that the primary unit sends gratuitous ARP packets. Gratuitous ARP packets are sent when a cluster unit becomes a primary unit (this can occur when the cluster is starting up or after a failover). The range is 1 to 60. | 5 |
| arps-interval <interval_integer> | Set the number of seconds to wait between sending gratuitous ARP packets. When a cluster unit becomes a primary unit (this occurs when the cluster is starting up or after a failover) the primary unit sends gratuitous ARP packets immediately to inform connected network equipment of the IP address and MAC address of the primary unit. The range is 1 to 20 seconds. | 8 |
| authentication { enable disable } | Enable/disable HA heartbeat message authentication using SHA1. | disable |
| cpu-threshold <weight_int> <low_int> <high_int> | Configure dynamic weighted load balancing for CPU usage. When enabled fewer sessions will be load balanced to the cluster unit when the CPU usage reaches the high watermark <high_int>. This is available when mode is a-a and schedule is weight-round-robin. Default low and high watermarks of 0 disable the feature. This setting is not synchronized by HA. | 5 0 0 |
| encryption { enable disable } | Enable/disable HA heartbeat message encryption using AES-128 for encryption and SHA1 for authentication. | disable |
| ftp-proxy-threshold <weight_int> <low_int> <high_int> | Configure dynamic weighted load balancing for FTP proxy sessions processed by a cluster unit. When enabled fewer sessions will be load balanced to the cluster unit when the high watermark <high_int> is reached. This is available when mode is a-a and schedule is weight-round-robin. Default low and high watermarks of 0 disable the feature. This setting is not synchronized by HA. | 5 0 0 |
| gratuitous-arps { enable disable } | Enable or disable gratuitous ARP packets from new master unit. These ARP packets are not needed if link-failed-signal is enabled. | enable |
| group-id <id_integer> | The HA group ID. The group ID range is from 0 to 255. All members of the HA cluster must have the same group ID. Changing the Group ID changes the cluster virtual MAC address. | 0 |
| group-name <name_str> | The HA group name. All cluster members must have the same group name. The maximum length of the group name is 32 characters. | FGT-HA |

| Variable | Description | Default |
|---|--|---------------------------------|
| ha-eth-type <type_int> | Set the Ethertype used by HA heartbeat packets for NAT/Route mode clusters. <type_int> is a 4-digit number. | 8890 |
| ha-mgmt-status {enable disable} | Enable or disable the HA reserved management interface feature. | disable |
| ha-mgmt-interface <interface_name> | Configure the FortiGate interface to be the reserved HA management interface. You can configure the IP address and other settings for this interface using the config system interface command. When you enable the reserved management interface feature the configuration of the reserved interface is not synchronized by HA. | No default. |
| ha-mgmt-interface-gateway <gateway_interface> | Configure the default route for the reserved HA management interface. This setting is not synchronized by HA. | 0.0.0.0 |
| ha-uptime-diff-margin <diff_int> | Change the cluster age difference margin (grace period). This margin is the age difference ignored by the cluster when selecting a primary unit based on age. Normally the default value of 300 seconds (5 minutes) should not be changed. However, for demo purposes you can use this option to lower the difference margin. | 300 |
| hb-interval <interval_integer> | The heartbeat interval is the time between sending heartbeat packets. The heartbeat interval range is 1 to 20 (100*milliseconds). So an hb-interval of 2 means a heartbeat packet is sent every 200 milliseconds. | 2 |
| hb-lost-threshold <threshold_integer> | The lost heartbeat threshold is the number of consecutive heartbeat packets that are not received from another cluster unit before assuming that the cluster unit has failed. The range is 1 to 60 packets. | 6 |
| hbdev <interface_name> <priority_integer> [<interface_name> <priority_integer>]... | Select the FortiGate interfaces to be heartbeat interfaces and set the heartbeat priority for each interface. The heartbeat interface with the highest priority processes all heartbeat traffic. If two or more heartbeat interfaces have the same priority, the heartbeat interface that with the lowest hash map order value processes all heartbeat traffic. By default two interfaces are configured to be heartbeat interfaces and the priority for both these interfaces is set to 50. The heartbeat interface priority range is 0 to 512. You can select up to 8 heartbeat interfaces. This limit only applies to FortiGate units with more than 8 physical interfaces. | Depends on the FortiGate model. |
| hc-eth-type <type_int> | Set the Ethertype used by HA heartbeat packets for Transparent mode clusters. <type_int> is a 4-digit number. | 8891 |

| Variable | Description | Default |
|--|--|---------|
| helo-holddown <holddown_integer> | The hello state hold-down time, which is the number of seconds that a cluster unit waits before changing from hello state to work state. The range is 5 to 300 seconds. | 20 |
| http-proxy-threshold <weight_int> <low_int> <high_int> | Configure dynamic weighted load balancing for HTTP proxy sessions processed by a cluster unit. When enabled fewer sessions will be load balanced to the cluster unit when the high watermark <high_int> is reached. This is available when mode is a-a and schedule is weight-round-robin. Default low and high watermarks of 0 disable the feature. This setting is not synchronized by HA. | 5 0 0 |
| imap-proxy-threshold <weight_int> <low_int> <high_int> | Configure dynamic weighted load balancing for IMAP proxy sessions processed by a cluster unit. When enabled fewer sessions will be load balanced to the cluster unit when the high watermark <high_int> is reached. This is available when mode is a-a and schedule is weight-round-robin. Default low and high watermarks of 0 disable the feature. This setting is not synchronized by HA. | 5 0 0 |
| l2ep-eth-type <type_int> | Set the Ethertype used by HA telnet sessions between cluster units over the HA link. <type_int> is a 4-digit number. | 8893 |
| link-failed-signal {enable disable} | Enable or disable shutting down all interfaces (except for heartbeat device interfaces) of a cluster unit with a failed monitored interface for one second after a failover occurs. Enable this option if the switch the cluster is connected to does not update its MAC forwarding tables after a failover caused by a link failure. | disable |
| load-balance-all {enable disable} | Select the traffic that is load balanced by active-active HA. Enable to load balance TCP sessions and sessions for firewall policies that include UTM options. Disable to load balance only sessions for firewall policies that include UTM options. Available if mode is a-a. | disable |
| load-balance-udp {enable disable} | Load balance UTM traffic between FS-5203B and FG-5001B. | disable |
| memory-threshold <weight_int> <low_int> <high_int> | Configure dynamic weighted load balancing for memory usage. When enabled fewer sessions will be load balanced to the cluster unit when the memory usage reaches the high watermark <high_int>. This is available when mode is a-a and schedule is weight-round-robin. Default low and high watermarks of 0 disable the feature. This setting is not synchronized by HA. | 5 0 0 |

| Variable | Description | Default |
|--|---|-------------|
| minimum-worker-threshold <threshold_int> | <p>Used only in content-cluster inter-chassis mode. In inter-chassis mode HA takes the number of worker (non-5203B) blades in a chassis when electing an HA master. Blades in a chassis that has less than "minimum-worker-threshold" worker blades available will be ranked lower than blades in a chassis that meets or exceeds "minimum-worker-threshold".</p> <p>The default value of 1 effectively disables the threshold. The maximum value is 11.</p> | 1 |
| mode {a-a a-p standalone} | <p>Set the HA mode.</p> <p>Enter a-p to create an Active-Passive cluster.</p> <p>Enter a-a to create an Active-Active cluster.</p> <p>Enter standalone to disable HA.</p> <p>All members of an HA cluster must be set to the same HA mode.</p> <p>Not available if a FortiGate interface mode is set to dhcp or pppoe.</p> | standalone |
| monitor <interface_names> | <p>Enable or disable port monitoring for link failure. Port monitoring (also called interface monitoring) monitors FortiGate interfaces to verify that the monitored interfaces are functioning properly and connected to their networks.</p> <p>Enter the names of the interfaces to monitor. Use a space to separate each interface name. If you want to remove an interface from the list or add an interface to the list you must retype the list with the names changed as required.</p> <p>You can monitor physical interfaces, redundant interfaces, and 802.3ad aggregated interfaces but not VLAN subinterfaces, IPSec VPN interfaces, or switch interfaces.</p> <p>You can monitor up to 64 interfaces. This limit only applies to FortiGate units with more than 16 physical interfaces. In a multiple VDOM configuration you can monitor up to 64 interfaces per virtual cluster.</p> | No default. |
| nntp-proxy-threshold <weight_int> <low_int> <high_int> | <p>Configure dynamic weighted load balancing for NNTP proxy sessions processed by a cluster unit. When enabled fewer sessions will be load balanced to the cluster unit when the high watermark <high_int> is reached.</p> <p>This is available when mode is a-a and schedule is weight-round-robin. Default low and high watermarks of 0 disable the feature.</p> <p>This setting is not synchronized by HA.</p> | 5 0 0 |

| Variable | Description | Default |
|--|---|-------------|
| override {enable disable} | <p>Enable or disable forcing the cluster to renegotiate and select a new primary unit every time a cluster unit leaves or joins a cluster, changes status within a cluster, or every time the HA configuration of a cluster unit changes.</p> <p>Automatically changes to <code>enable</code> when you enable virtual cluster 2.</p> <p>This setting is not synchronized by HA.</p> | disable |
| password <password_str> | Enter a password for the HA cluster. The password must be the same for all FortiGate units in the cluster. The maximum password length is 15 characters. | No default. |
| pingserver-failover-threshold <threshold_integer> | <p>Set the HA remote IP monitoring failover threshold.</p> <p>The failover threshold range is 0 to 50. Setting the failover threshold to 0 means that if any ping server added to the HA remote IP monitoring configuration fails an HA failover will occur.</p> <p>Set the priority for each remote IP monitoring ping server using the <code>ha-priority</code> field of the command “router gwdetect” on page 369.</p> | 0 |
| pingserver-flip-timeout <timeout_integer> | Set the HA remote IP monitoring flip timeout in minutes. If HA remote IP monitoring fails on all cluster units because none of the cluster units can connect to the monitored IP addresses, the flip timeout stops a failover from occurring until the timer runs out. The range is 6 to 2147483647 minutes. | 60 |
| pingserver-monitor-interface <interface_names> | <p>Enable HA remote IP monitoring by specifying the FortiGate unit interfaces that will be used to monitor remote IP addresses. You can configure remote IP monitoring for all types of interfaces including physical interfaces, VLAN interfaces, redundant interfaces and aggregate interfaces.</p> <p>Use a space to separate each interface name. If you want to remove an interface from the list or add an interface to the list you must retype the list with the names changed as required.</p> | |
| pop3-proxy-threshold <weight_int> <low_int> <high_int> | <p>Configure dynamic weighted load balancing for POP3 proxy sessions processed by a cluster unit. When enabled fewer sessions will be load balanced to the cluster unit when the high watermark <code><high_int></code> is reached.</p> <p>This is available when <code>mode</code> is <code>a-a</code> and <code>schedule</code> is <code>weight-round-robin</code>. Default low and high watermarks of 0 disable the feature.</p> <p>This setting is not synchronized by HA.</p> | 5 0 0 |

| Variable | Description | Default |
|---|---|-------------|
| priority <priority_integer> | Change the device priority of the cluster unit. Each cluster unit can have a different device priority (the device priority is not synchronized among cluster members). During HA negotiation, the cluster unit with the highest device priority becomes the primary unit. The device priority range is 0 to 255. This setting is not synchronized by HA. | 128 |
| route-hold <hold_integer> | The minimum time between primary unit updates to the routing tables of subordinate units in a cluster. The route hold range is 0 to 3600 seconds. | 10 |
| route-ttl <ttl_integer> | The time to live for routes in a cluster unit routing table. The time to live range is 5 to 3600 seconds. The time to live controls how long routes remain active in a cluster unit routing table after the cluster unit becomes a primary unit. | 10 |
| route-wait <wait_integer> | The time the primary unit waits after receiving a routing table update before attempting to update the subordinate units in the cluster. The route-wait range is 0 to 3600 seconds. | 0 |
| schedule {hub ip ipport leastconnection none random round-robin weight-round-robin} | Active-active load balancing schedule. hub load balancing if the cluster interfaces are connected to hubs. Traffic is distributed to cluster units based on the Source IP and Destination IP of the packet. <ul style="list-style-type: none"> ip — load balancing according to IP address. ipport — load balancing according to IP address and port. leastconnection — least connection load balancing. none — no load balancing. Use none when the cluster interfaces are connected to load balancing switches. random — random load balancing. round-robin — round robin load balancing. If the cluster units are connected using switches, use round-robin to distribute traffic to the next available cluster unit. weight-round-robin — weighted round robin load balancing. Similar to round robin, but you can assign weighted values to each of the units in a cluster. | round-robin |

| Variable | Description | Default |
|---|---|-------------|
| session-pickup {enable disable} | <p>Enable or disable session pickup. Enable <code>session-pickup</code> so that if the primary unit fails, all sessions are picked up by the new primary unit.</p> <p>If you enable session pickup the subordinate units maintain session tables that match the primary unit session table. If the primary unit fails, the new primary unit can maintain all active communication sessions.</p> <p>If you do not enable session pickup the subordinate units do not maintain session tables. If the primary unit fails all sessions are interrupted and must be restarted when the new primary unit is operating.</p> | disable |
| session-pickup-connectionless {enable disable} | Enable or disable session synchronization for connectionless (UDP and ICMP) sessions when mode is set to a-a or a-p. When mode is standalone, FGSP cluster session pickup applies to TCP session synchronization only. This is available if <code>session-pickup</code> is enabled. | disable |
| session-pickup-delay {enable disable} | Enable to synchronize sessions only if they remain active for more than 30 seconds. This option improves performance when <code>session-pickup</code> is enabled by reducing the number of sessions that are synchronized. | disable |
| session-pickup-expectation {enable disable} | Enable or disable session synchronization for expectation sessions in an FGSP cluster. This is available if <code>session-pickup</code> is enabled and mode is standalone. | disable |
| session-pickup-nat {enable disable} | Enable or disable session synchronization for NAT sessions in an FGSP cluster. This is available if <code>session-pickup</code> is enabled. This is available if <code>session-pickup</code> is enabled and mode is standalone.. | disable |
| session-sync-daemon-number <process_id_int> | Set the number of processes used by the HA session sync daemon. Increase the number of processes to handle session packets sent from the kernel efficiently when the session rate is high. Intended for ELBC clusters, this feature only works for clusters with two members. Range 1 to 15. | 1 |
| session-sync-dev <interface_name> [<interface_name>]... | Select FortiGate interfaces to be used for session synchronization between cluster units instead of using the heartbeat interface. You can select up to 8 session synchronization interfaces. Session synchronization packets are load balanced among these interfaces. | No default. |
| slave-switch-standby {enable disable} | Enable to force slave FS-5203B into standby mode even though its weight is non-zero. | disable |

| Variable | Description | Default |
|--|--|---------|
| smtp-proxy-threshold <weight_int> <low_int> <high_int> | <p>Configure dynamic weighted load balancing for SMTP proxy sessions processed by a cluster unit. When enabled fewer sessions will be load balanced to the cluster unit when the high watermark <high_int> is reached.</p> <p>This is available when mode is a-a and schedule is weight-round-robin. Default low and high watermarks of 0 disable the feature.</p> <p>This setting is not synchronized by HA.</p> | 5 0 0 |
| standalone-config-sync {enable disable} | Synchronize the configuration of the FortiGate units in an FGSP cluster. This is available if session-pickup is enabled and mode is standalone. | disable |
| sync-config {enable disable} | Enable or disable automatic synchronization of primary unit configuration changes to all cluster units. | enable |
| uninterruptible-upgrade {enable disable} | <p>Enable or disable upgrading the cluster without interrupting cluster traffic processing.</p> <p>If uninterruptible-upgrade is enabled, traffic processing is not interrupted during a normal firmware upgrade. This process can take some time and may reduce the capacity of the cluster for a short time.</p> <p>If uninterruptible-upgrade is disabled, traffic processing is interrupted during a normal firmware upgrade (similar to upgrading the firmware operating on a standalone FortiGate unit).</p> | enable |
| update-all-session-timer {enable disable} | Enable or disable updating all session timers after a failover. | disable |

| Variable | Description | Default |
|---|---|---|
| weight <priority_integer> <weight_integer> | <p>The weighted round robin load balancing weight to assign to each cluster unit in an active-active cluster. When you set <code>schedule</code> to <code>weight-round-robin</code> you can use the <code>weight</code> field to set the weight of each cluster unit. The weight is set according to the priority of the unit in the cluster. A FortiGate HA cluster can contain up to 4 FortiGate units so you can set up to 4 weights.</p> <p>The default weight means that the 4 possible units in the cluster all have the same weight of 40. The cluster units are numbered 0 to 3.</p> <p><code>priority_integer</code> is a number from 0 to 3 that identifies the priority of the cluster unit.</p> <p><code>weight-integer</code> is a number between 0 and 255 that is the weight assigned to the cluster units according to their priority in the cluster. Increase the weight to increase the number of connections processed by the cluster unit with that priority.</p> <p>You enter the weight for each unit separately. For example, if you have a cluster of 4 FortiGate units you can set the weights for each unit as follows:</p> <pre>set weight 0 5 set weight 1 10 set weight 2 15 set weight 3 20</pre> | |
| vdom <vdom_names> | <p>Add virtual domains to virtual cluster 1 or virtual cluster 2. Virtual cluster 2 is also called the secondary virtual cluster.</p> <p>In the <code>config system ha</code> shell, use <code>set vdom</code> to add virtual domains to virtual cluster 1. Adding a virtual domain to virtual cluster 1 removes that virtual domain from virtual cluster 2.</p> <p>In the <code>config secondary-vcluster</code> shell, use <code>set vdom</code> to add virtual domains to virtual cluster 2. Adding a virtual domain to virtual cluster 2 removes it from virtual cluster 1.</p> <p>You can use <code>vdom</code> to add virtual domains to a virtual cluster in any combination. You can add virtual domains one at a time or you can add multiple virtual domains at a time. For example, entering <code>set vdom domain_1</code> followed by <code>set vdom domain_2</code> has the same result as entering <code>set vdom domain_1 domain_2</code>.</p> | All virtual domains are added to virtual cluster 1. |

| Variable | Description | Default |
|--|---|---|
| vcluster2 {disable enable} | <p>Enable or disable virtual cluster 2.</p> <p>When multiple VDOMs are enabled, virtual cluster 2 is enabled by default. When virtual cluster 2 is enabled you can use <code>config secondary-vcluster</code> to configure virtual cluster 2.</p> <p>Disable virtual cluster 2 to move all virtual domains from virtual cluster 2 back to virtual cluster 1.</p> <p>Enabling virtual cluster 2 enables <code>override</code> for virtual cluster 1 and virtual cluster 2.</p> | <p>disable</p> <p>enable when multiple VDOMs are enabled</p> |
| config secondary-vcluster | <p>Configure virtual cluster 2. You must enable <code>vcluster2</code>. Then you can use <code>config secondary-vcluster</code> to set <code>monitor</code>, <code>override</code>, <code>priority</code>, and <code>vdom</code> for virtual cluster 2.</p> <p><code>priority</code> setting is not synchronized by HA.</p> | <p>Same defaults as virtual cluster 1 except that the default value for <code>override</code> is <code>enable</code>.</p> |
| config frup-settings fields These fields configure the Fortinet Redundant UTM Protocol (FRUP). | | |
| active-interface <interface_name> | Select active interface. | No default. |
| backup-interface <interface_name> | Select backup interface. | No default. |
| active-switch-port <port_number> | Enter active switch port. | No default. |

interface

Use this command to edit the configuration of a FortiGate physical interface, VLAN subinterface, IEEE 802.3ad aggregate interface, redundant interface, or IPSec tunnel interface.

In the following table, VLAN subinterface can be substituted for interface in most places except that you can only configure VLAN subinterfaces with static IP addresses. Use the edit command to add a VLAN subinterface.



VLAN communication over the backplane interfaces is available for FortiGate-5000 modules installed in a FortiGate-5020 chassis. The FortiSwitch-5003 does not support VLAN-tagged packets so VLAN communication is not available over the FortiGate-5050 and FortiGate-5140 chassis backplanes.

Some fields are specific to aggregate interfaces. These appear at the end of the list of commands under [“variables for aggregate and redundant interfaces \(some FortiGate models\)” on page 578](#).

Some FortiGate models have multiple interfaces that are grouped as a switch named “internal”. This is switch mode and it is the default. As an alternative, you can select interface mode to use each interface independently. For more information, see [internal-switch-mode](#) in [“system global” on page 523](#).

Using the one-arm intrusion detection system (IDS), you can now configure a FortiGate unit to operate as an IDS appliance by sniffing packets for attacks without actually receiving and otherwise processing the packets. For more information, see the [ips-sniffer-mode {enable | disable}](#) field.

An interface’s IPv6 address can be included in a Multi Listener Discovery (MLD) report. By default the FortiGate unit includes no addresses in the MLD report. For more information, see the [ip6-send-adv {enable | disable}](#) field.

Syntax

Entering a name string for the `edit` field that is not the name of a physical interface adds a VLAN subinterface.

```
config system interface
  edit <interface_name>
    set allowaccess <access_types>
    set alias <name_string>
    set arpforward {enable | disable}
    set atm-protocol {ipoa | none}
    set auth-type <ppp_auth_method>
    set bfd {enable | disable | global}
    set bfd-desired-min-tx <interval_msec>
    set bfd-detect-mult <multiplier>
    set bfd-required-min-rx <interval_msec>
    set broadcast-forward {enable | disable}
    set defaultgw {enable | disable}
    set dedicated-to {management | none}
    set description <text>
    set device-access-list <list_name>
    set device-identification {enable | disable}
    set device-netscan {enable | disable}
```

```
set device-user-identification {enable | disable}
set dhcp-client-identifier <client_name_str>
set dhcp-relay-ip <dhcp_relay1_ipv4> {... <dhcp_relay8_ipv4>}
set dhcp-relay-service {enable | disable}
set dhcp-relay-type {ipsec | regular}
set disc-retry-timeout <pppoe_retry_seconds>
set distance <admin_distance>
set dns-server-override {enable | disable}
set drop-fragment {enable | disable}
set drop-overlapped-fragment {enable | disable}
set elbc-default-gw <ipv4_addr>
set explicit-ftp-proxy {enable | disable}
set explicit-web-proxy {enable | disable}
set external {enable | disable}
set fail-detect {enable | disable}
set fail-detect-option {link-down | detectserver}
set fail-alert-method {link-down | link-failed-signal}
set fail-alert-interfaces {port1 port2 ...}
set forward-domain <collision_group_number>
set fp-anomaly [...]
set gi-gk {enable | disable}
set icmp-redirect {enable | disable}
set ident-accept {enable | disable}
set idle-timeout <pppoe_timeout_seconds>
set inbandwidth <bandwidth_integer>
set interface <port_name>
set ip <interface_ipv4mask>
set ipmac {enable | disable}
set ips-sniffer-mode {enable | disable}
set ipunnumbered <unnumbered_ipv4>
set l2forward {enable | disable}
set l2tp-client {enable | disable}
set lacp-ha-slave {enable | disable}
set lacp-mode {active | passive | static}
set lacp-speed {fast | slow}
set lcp-echo-interval <lcp_interval_seconds>
set lcp-max-echo-fails <missed_echoes>
set listen-forticlient-connection {enable | disable}
set macaddr <mac_address>
set mediatype {serdes-sfp | sgmii-sfp}
set member <if_name1> <if_name2> ...
set mode <interface_mode>
set mtu <mtu_bytes>
set mtu-override {enable | disable}
set netbios-forward {disable | enable}
set nonntp-web-proxy {disable | enable}
set outbandwidth <bandwidth_integer>
```

```
set padt-retry-timeout <padt_retry_seconds>
set password <pppoe_password>
set pbx-user-portal {enable | disable}
set phone-auto-provision {enable | disable}
set poe {disable | enable}
set polling-interval <interval_int>
set pppoe-unnumbered-negotiate {disable | enable}
set pptp-client {disable | enable}
set pptp-user <pptp_username>
set pptp-password <pptp_userpassword>
set pptp-server-ip <pptp_serverid>
set pptp-auth-type <pptp_authtype>
set pptp-timeout <pptp_idletimeout>
set priority <learned_priority>
set remote-ip <ipv4>
set replacemsg-override-group {group-name}
set sample-direction {both | rx | tx}
set sample-rate <rate_int>
set secondary-IP {enable | disable}
set security-groups [group1 [group2 ... groupn]]}
set security-mode {none | captive-portal | 802.1X}
set sflow-sampler {disable | enable}
set snmp-index <id_int>
set speed <interface_speed>
set spillover-threshold <threshold_int>
set status {down | up}
set stpforward {enable | disable}
set stpforward-mode {rpl-all-ext-id | rpl-bridge-ext-id
    | rpl-nothing}
set subst {enable | disable}
set substitute-dst-mac <destination_mac_addres>
set tcp-mss <max_send_bytes>
set trust-ip-1 <ipmask>
set trust-ip-2 <ipmask>
set trust-ip-3 <ipmask>
set type {aggregate | hard-switch | hdlc | loopback | physical |
    redundant | tunnel | vap-switch | vdom-link | vlan |
    wireless}
set username <pppoe_username>
set vdom <vdom_name>
set vlanforward {enable | disable}
set vlanid <id_number>
set voip {enable | disable}
set vrrp-virtual-mac {enable | disable}
set wccp {enable | disable}
set weight <int>
set wifi-acl {allow | deny}
set wifi-auth {PSK | radius | usergroup}
set wifi-broadcast-ssid {enable | disable}
```

```
set wifi-encrypt {AES | TKIP}
set wifi-fragment_threshold <packet_size>
set wifi-key <hex_key>
set wifi-mac-filter {enable | disable}
set wifi-passphrase <pass_str>
set wifi-radius-server <server_name>
set wifi-rts_threshold <integer>
set wifi-security <sec_mode>
set wifi-ssid <id_str>
set wifi-auto-connect {enable | disable}
set wifi-auto-save {enable | disable}
set wins-ip <wins_server_ip>
config ipv6
    set autoconf {enable | disable}
    set dhcp6-relay-server {enable | disable}
    set dhcp6-relay-ip {ip1_ipv6 ... ipn_ipv6}
    set ip6-address <if_ipv6mask>
    set ip6-allowaccess <access_types>
    set ip6-default-life <ipv6_life_seconds>
    set ip6-hop-limit <ipv6_hops_limit>
    set ip6-link-mtu <ipv6_mtu>
    set ip6-manage-flag {disable | enable}
    set ip6-max-interval <adverts_max_seconds>
    set ip6-min-interval <adverts_min_seconds>
    set ip6-mode {static | dhcp6 | pppoe}
    set ip6-other-flag {enable | disable}
    set ip6-reachable-time <reachable_msecs>
    set ip6-retrans-time <retrans_msecs>
    set ip6-send-adv {enable | disable}
    config ip6-prefix-list
        edit <ipv6_prefix>
            set autonomous-flag {enable | disable}
            set onlink-flag {enable | disable}
            set preferred-life-time <seconds>
            set valid-life-time <seconds>
        end
    end
```

```
end
config ip6-extra-address
    edit <prefix_ipv6>
end
end
config l2tp-client-settings
    set auth-type {auto | chap | mschapv1 | mschapv2 | pap}
    set defaultgw {enable | disable}
    set distance <admin_distance>
    set mtu <integer>
    set password <password>
    set peer-host <ipv4_addr>
    set peer-mask <netmask>
    set peer-port <port_num>
    set priority <integer>
    set user <string>
end
config secondaryip
    edit <secondary_ip_id>
        set allowaccess <access_types>
        set ip <interface_ipv4mask>
    end
end
config vrrp
    edit <VRID_int>
        set adv-interval <seconds_int>
        set preempt {enable | disable}
        set priority <prio_int>
        set start-time <seconds_int>
        set status {enable | disable}
        set vrdest <ipv4_addr>
        set vrip <ipv4_addr>
    end
config wifi-mac_list
    edit <entry_number>
        set mac <mac_address>
    end
config wifi-networks
    edit <network_id>
        set wifi-key <key_str>
        set wifi-keyindex <index_int>
        set wifi-passphrase <psk_str>
        set wifi-security {wpa-personal | wep128 | wep64 | open}
        set wifi-ssid <ssid_str>
    end
end
```



A VLAN cannot have the same name as a zone or a virtual domain.

| Variable | Description | Default |
|----------------------------------|--|----------------------------|
| allowaccess <access_types> | <p>Enter the types of management access permitted on this interface or secondary IP address. Separate types with spaces. Use the append or clear commands (instead of set) to add or remove an option from the list.</p> <p>Valid types are:</p> <p>auto-ipsec — required for IPsec auto-configuration</p> <p>capwap — required for interfaces that carry CAPWAP control traffic. Interfaces dedicated for FortiAP unit use have this option enabled automatically.</p> <p>fgfm — FortiManager management access</p> <p>http — enable HTTP admin access</p> <p>https — enable HTTPS admin access</p> <p>ping — allow ping response. Useful for testing.</p> <p>probe-response — allow access by config system server-probe command</p> <p>radius-acct — RADIUS Accounting server access</p> <p>snmp — SNMP management access</p> <p>ssh — enable admin access via SSH</p> <p>telnet — enable admin access via Telnet</p> | Varies for each interface. |
| alias <name_string> | <p>Enter an alias name for the interface. Once configured, the alias will be displayed with the interface name to make it easier to distinguish. The alias can be a maximum of 25 characters.</p> <p>This option is only available when interface type is physical.</p> | |
| arpforward {enable disable} | <p>Enable or disable forwarding of ARP packets on this interface.</p> <p>ARP forwarding is required for DHCP relay and MS Windows Client browsing.</p> | enable |
| atm-protocol {ipoa none} | Enable IPoA protocol. This is available on ADSL interfaces that support IPoA. | none |

| Variable | Description | Default |
|---|--|-------------|
| auth-type <ppp_auth_method> | <p>Select the PPP authentication method for this interface. Choose one of:</p> <p>auto — select authentication method automatically</p> <p>chap — CHAP</p> <p>mschapv1 — Microsoft CHAP v1</p> <p>mschapv2 — Microsoft CHAP v2</p> <p>pap — PAP</p> <p>This is available only when mode is pppoe, and type of interface is physical.</p> | auto |
| bfd {enable disable global} | <p>The status of Bidirectional Forwarding Detection (bfd) on this interface:</p> <p>enable — enable BFD and ignore global BFD configuration.</p> <p>disable — disable BFD on this interface.</p> <p>global — use the BFD configuration in <code>system settings</code> for the virtual domain to which this interface belongs.</p> <p>The BFD-related fields below are available only if <code>bfd</code> is enabled.</p> | global |
| bfd-desired-min-tx <interval_msec> | <p>Enter the minimum desired interval for the BFD transmit interval. Valid range is from 1 to 100 000 msec.</p> <p>This is available only if <code>bfd</code> is enable.</p> | 50 |
| bfd-detect-mult <multiplier> | <p>Select the BFD detection multiplier.</p> <p>This is available only if <code>bfd</code> is enable.</p> | 3 |
| bfd-required-min-rx <interval_msec> | <p>Enter the minimum required interface for the BFD receive interval. Valid range is from 1 to 100 000 msec.</p> <p>This is available only if <code>bfd</code> is enable.</p> | 50 |
| broadcast-forward {enable disable} | <p>Select to enable automatic forwarding of broadcast packets.</p> <p>Use with caution. Enabling this option may make the FortiGate unit vulnerable to broadcast-based DoS attacks such as ping floods.</p> | disable |
| defaultgw {enable disable} | <p>Enable to get the gateway IP address from the DHCP or PPPoE server.</p> <p>This is valid only when the mode is one of DHCP or PPPoE.</p> | disable |
| dedicated-to {management none} | <p>Select whether this port is dedicated to unit management or not. This is available on “mgmt” ports where mode is static.</p> | none |
| description <text> | <p>Optionally, enter up to 63 characters to describe this interface.</p> | No default. |

| Variable | Description | Default |
|--|--|-------------|
| device-access-list <list_name> | Enter the device access list to use. The device access list is configured in user device-access-list . This field is available when <code>device-identification</code> is enabled. | No default. |
| device-identification {enable disable} | Enable to attempt to discover OS and device information for source hosts. | disable |
| device-netscan {enable disable} | Enable to include detected devices in network vulnerability scans. This is available if <code>device-identification</code> is enabled. | disable |
| device-user-identification {enable disable} | Enable to attempt to determine user name for source hosts. | enable |
| dhcp-client-identifier <client_name_str> | <p>Override the default DHCP client identifier used by this interface. The DHCP client identifier is used by DHCP to identify individual DHCP clients (in this case individual FortiGate interfaces).</p> <p>By default the DHCP client identifier for each FortiGate interface is created based on the FortiGate model name and the interface MAC address. In some cases you may want to specify your own DHCP client identifier using this command.</p> <p>This is available if <code>mode</code> is set to <code>dhcp</code>.</p> | |
| dhcp-relay-ip <dhcp_relay1_ipv4> {... <dhcp_relay8_ipv4>} | <p>Set DHCP relay IP addresses. You can specify up to eight DHCP relay servers for DHCP coverage of subnets.</p> <p>Generally, clients respond to the first offer they receive. The relay agent broadcasts back the DHCPREQUEST and ACKNOWLEDGE messages so that other DHCP servers do not reserve the addresses they offered.</p> <p>Do not set <code>dhcp-relay-ip</code> to 0.0.0.0.</p> | No default. |
| dhcp-relay-service {enable disable} | <p>Enable to provide DHCP relay service on this interface. The DHCP type relayed depends on the setting of <code>dhcp-relay-type</code>.</p> <p>There must be no other DHCP server of the same type (regular or ipsec) configured on this interface.</p> | disable |
| dhcp-relay-type {ipsec regular} | Set <code>dhcp_type</code> to <code>ipsec</code> or <code>regular</code> depending on type of firewall traffic. | regular |
| disc-retry-timeout <pppoe_retry_seconds> | <p>Set the initial PPPoE discovery timeout in seconds. This is the time to wait before retrying to start a PPPoE discovery. Set to 0 to disable this feature.</p> <p>This field is only available in NAT/Route mode when <code>mode</code> is set to <code>pppoe</code>.</p> | 1 |

| Variable | Description | Default |
|--|--|-----------|
| distance <admin_distance> | Configure the administrative distance for routes learned through PPPoE or DHCP. Use the administrative distance to specify the relative priorities of different routes to the same destination. A lower administrative distance indicates a more preferred route. Distance can be an integer from 1-255. For more information, see router static “distance <distance>” on page 447 This variable is only available in NAT/Route mode when mode is set to dhcp or pppoe. | 1 |
| dns-server-override {enable disable} | Disable to prevent this interface from using DNS server addresses it acquires via DHCP or PPPoE. This variable is only displayed if mode is set to dhcp or pppoe. | enable |
| drop-fragment {enable disable} | Enable to drop fragmented packets log them as invalid. | disable |
| drop-overlapped-fragment {enable disable} | Enable or disable dropping overlapped packet fragments. | disable |
| edit <interface_name> | Edit an existing interface or create a new VLAN interface. | None. |
| edit <ipv6_prefix> | Enter the IPv6 prefix you want to configure. For settings, see the edit <ipv6_prefix> variables section of this table. | None. |
| edit <secondary_ip_id> | Enter an integer identifier, e.g., 1, for the secondary ip address that you want to configure. | None. |
| elbc-default-gw <ipv4_addr> | Use to add a default gateway to hidden front panel ports in ELBC mode. When in ELBC mode the front panel ports are placed in a secret hidden VDOM. This prevents the user from adding routes to that interface. Using the elbc-default-gw attribute present on front panel ports the user can add a default gateway to these interfaces. | |
| explicit-ftp-proxy {enable disable} | Enable explicit FTP proxy on this interface. For more information, see “explicit” on page 252 . | disable |
| explicit-web-proxy {enable disable} | Enable explicit Web proxy on this interface. For more information, see “explicit” on page 877 . | disable |
| external {enable disable} | Enable to indicate that an interface is an external interface connected to an external network. This option is used for SIP NAT when the config VoIP profile SIP contact-fixup option is disabled. | disable |
| fail-detect {enable disable} | Enable interface failure detection. | disable |
| fail-detect-option {link-down detectserver} | Select whether the FortiGate unit detects interface failure by port detection (link-down) or ping server (detectserver). detectserver is only available in NAT mode. | link-down |

| Variable | Description | Default |
|--|--|---------------------------------|
| fail-alert-method {link-down link-failed-signal} | Select the signal that the FortiGate unit uses to signal the link failure: Link Down or Link Failed. | link-down |
| fail-alert-interfaces {port1 port2 ...} | Select the interfaces to which failure detection applies. | |
| forward-domain <collision_group_number> | Specify the collision domain to which this interface belongs. Layer 2 broadcasts are limited to the same group. By default, all interfaces are in group 0. Collision domains prevent the forwarding of ARP packets to all VLANs on an interface. Without collision domains, duplicate MAC addresses on VLANs may cause ARP packets to be duplicated. Duplicate ARP packets can cause some switches to reset. This command is only available in Transparent mode. | 0 |
| fp-anomaly [...] | Enable NP2 hardware fast path anomaly checking on an interface and specify whether to drop or allow (pass) different types of anomalies. When no options are specified, anomaly checking performed by the network processor is disabled. If pass options are specified, packets may still be rejected by other anomaly checks, including policy-required IPS performed using the FortiGate unit main processing resources. Log messages are generated when packets are dropped due to options in this setting. The fp-anomaly option is available for NP2-enabled interfaces. | No options specified (disabled) |
| gi-gk {enable disable} | Enable FortiOS Carrier Gi Gatekeeper to enable the Gi firewall on this interface as part of the anti-overbilling configuration. | disable |
| icmp-redirect {enable disable} | Disable to stop ICMP redirect from sending from this interface. ICMP redirect messages are sent by a router to notify the original sender of packets that there is a better route available. | enable |
| ident-accept {enable disable} | Enable or disable passing ident packets (TCP port 113) to the firewall policy. If set to disable, the FortiGate unit sends a TCP reset packet in response to an ident packet. | disable |
| idle-timeout <pppoe_timeout_seconds> | Disconnect if the PPPoE connection is idle for the specified number of seconds. Set to zero to disable this feature. This is available when mode is set to pppoe. | 0 |

| Variable | Description | Default |
|--|---|----------------------------|
| inbandwidth <bandwidth_integer> | <p>Enter the Kbit/sec limit for incoming traffic for this interface.</p> <p>Use this command to configure inbound traffic shaping for an interface. Inbound traffic shaping limits the bandwidth accepted by the interface. Limiting inbound traffic takes precedence over traffic shaping applied by firewall policies.</p> <p>You can set inbound traffic shaping for any FortiGate unit interface and it can be active for more than one FortiGate unit interface at a time. Setting <bandwidth_integer> to 0 (the default) means unlimited bandwidth or no traffic shaping.</p> <p>This does not affect traffic offloaded to NP2, NP4 and SP3 processors.</p> | 0 |
| interface <port_name> | <p>Enter the physical or VAP interface this virtual interface is linked to.</p> <p>This is available only when adding virtual interfaces such as VLANs and VPNs.</p> | None. |
| ip <interface_ipv4mask> | <p>Enter the interface IP address and netmask.</p> <p>This is not available if mode is set to dhcp or pppoe. You can set the IP and netmask, but it will not display.</p> <p>This is only available in NAT/Route mode.</p> <p>The IP address cannot be on the same subnet as any other FortiGate unit interface.</p> | Varies for each interface. |
| ipmac {enable disable} | <p>Enable or disable IP/MAC binding for the specified interface. For information about configuring IP/MAC binding settings, see “ipmacbinding setting” on page 139 and “ipmacbinding table” on page 140.</p> | disable |
| ips-sniffer-mode {enable disable} | <p>Enable to configure this interface to operate as a one-armed sniffer as part of configuring a FortiGate unit to operate as an IDS appliance by sniffing packets for attacks without actually receiving and otherwise processing the packets. Once the interface is enabled for sniffing you cannot use the interface for other traffic. You must add sniffer policies for the interface to actually sniff packets.</p> <p>For more information on one-armed IPS, see “firewall sniff-interface-policy” on page 214 and “firewall sniff-interface-policy6” on page 217.</p> | disable |

| Variable | Description | Default |
|---|---|-------------|
| ipunnumbered <unnumbered_ipv4> | <p>Enable IP unnumbered mode for PPPoE. Specify the IP address to be borrowed by the interface. This IP address can be the same as the IP address of another interface or can be any IP address.</p> <p>This is only available when <code>mode</code> is <code>pppoe</code>.</p> <p>The Unnumbered IP may be used for PPPoE interfaces for which no unique local address is provided. If you have been assigned a block of IP addresses by your ISP for example, you can add any of these IP addresses to the Unnumbered IP.</p> | No default. |
| l2forward {enable disable} | <p>Enable to allow layer-2 forwarding for this interface.</p> <p>If there are layer-2 protocols such as IPX, PPTP or L2TP in use on your network, you need to configure your FortiGate unit interfaces to pass these protocols without blocking.</p> <p>Enabling <code>l2forward</code> may cause packets to repeatedly loop through the network, much like a broadcast storm. In this case either disable <code>l2forward</code>, or enable Spanning Tree Protocol (STP) on your network's switches and routers.</p> <p>For more information, see FortiGate VLANs and VDOMs.</p> | disable |
| l2tp-client {enable disable} | <p>Enable or disable this interface as a Layer 2 Tunneling Protocol (L2TP) client.</p> <p>Enabling makes config l2tp-client-settings visible.</p> <p>You may need to enable <code>l2forward</code> on this interface.</p> <p>This is available only on FortiGate 50 series, 60 series, and 100A.</p> <p>The interface can not be part of an aggregate interface, and the FortiGate unit can not be in Transparent mode, or HA mode. If <code>l2tp-client</code> is enabled on an interface, the FortiGate unit will not enter HA mode until the L2TP client is disabled.</p> | disable |
| lcp-echo-interval <lcp_interval_seconds> | <p>Set the interval in seconds between PPPoE Link Control Protocol (LCP) echo requests.</p> <p>This is available only when <code>mode</code> is <code>pppoe</code>.</p> | 5 |
| lcp-max-echo-fails <missed_echoes> | <p>Set the maximum number of missed LCP echoes before the PPPoE link is disconnected.</p> <p>This is only available when <code>mode</code> is <code>pppoe</code>.</p> | 3 |
| listen-forticlient-connection {enable disable} | <p>Enable listening for FortiClient endpoints connecting. This is required for endpoint compliance on endpoints that are connected to the interface through a router.</p> <p><code>listen-forticlient-connection</code> must be configured on the internal interface and on the IPsec tunnel interface if connection is via VPN.</p> | disable |

| Variable | Description | Default |
|------------------------------------|---|--------------|
| macaddr <mac_address> | Override the factory set MAC address of this interface by specifying a new MAC address. Use the form xx:xx:xx:xx:xx:xx. This is only used for physical interfaces. | Factory set. |
| mediatype {serdes-sfp sgmii-sfp} | Some FortiGate SFP interfaces can operate in SerDes (Serializer/Deserializer) or SGMII (Serial Gigabit Media Independent Interface) mode. The mode that the interface operates in depends on the type of SFP transceiver installed. Use this field to switch the interface between these two modes. Set mediatype to: serdes-sfp if you have installed a SerDes transceiver. In SerDes mode an SFP interface can only operate at 1000 Mbps. sgmii-sfp if you have installed an SGMII transceiver. In SGMII mode the interface can operate at 10, 100, or 1000 Mbps. This field is available for some FortiGate SFP interfaces. For example, all FortiGate-ASM-FB4 interfaces and interfaces port3 to port18 of the FortiGate-3016B support both SerDes and SGMII mode. | serdes-sfp |
| mode <interface_mode> | Configure the connection mode for the interface as one of: static — configure a static IP address for the interface. dhcp — configure the interface to receive its IP address from an external DHCP server. pppoe — configure the interface to receive its IP address from an external PPPoE server. This is available only in NAT/Route mode. eoat — Ethernet over ATM pppoeat — IP over ATM (also known as bridged mode). This variable is only available in NAT/Route mode. | static |

| Variable | Description | Default |
|---------------------------------------|---|---------|
| mtu <mtu_bytes> | <p>Set a custom maximum transmission unit (MTU) size in bytes. Ideally set <code>mtu</code> to the size of the smallest MTU of all the networks between this FortiGate unit and the packet destination.</p> <p><mtu_bytes> valid ranges are:</p> <ul style="list-style-type: none"> • 68 to 1 500 bytes in <code>static</code> mode • 576 to 1 500 bytes in <code>dhcp</code> mode • 576 to 1 492 bytes in <code>pppoe</code> mode • up to 9 000 bytes for NP2-accelerated interfaces • over 1 500 bytes on high end FortiGate models on some interfaces. <p>If you enter an MTU that is not supported, an error message informs you of the valid range for this interface.</p> <p>In Transparent mode, if you change the MTU of an interface, you must change the MTU of all interfaces to match the new MTU.</p> <p>If you configure an MTU size larger than 1 500 on your FortiGate unit, all other network equipment on the route to the destination must also support that frame size.</p> <p>You can set the MTU of a physical interface, a VLAN interface, and some tunnel interfaces (not IPsec). All virtual interfaces inherit the MTU of the parent physical interface.</p> <p>The variable <code>mtu</code> is only available when <code>mtu-override</code> is enabled.</p> | 1 500 |
| mtu-override {enable disable} | <p>Select enable to use custom MTU size instead of default (1 500). This is available only for physical interfaces and some tunnel interfaces (not IPsec).</p> <p>Some models support MTU sizes larger than the standard 1 500 bytes.</p> | disable |
| netbios-forward {disable enable} | <p>Enable to forward Network Basic Input/Output System (NetBIOS) broadcasts to a Windows Internet Name Service (WINS) server. Use wins-ip <wins_server_ip> to set the WINS server IP address.</p> <p>This variable is only available in NAT/Route mode.</p> | disable |
| nontp-web-proxy {disable enable} | <p>Enable to turn on web cache support for this interface, such as accepting HTTP proxies and DNS requests. Web caching accelerates web applications and web servers by reducing bandwidth usage, server load, and perceived latency. For more information, see “web-proxy explicit” on page 877.</p> <p>This variable is only available when this interface is in NAT/Route mode.</p> | disable |

| Variable | Description | Default |
|--|---|-------------|
| outbandwidth <bandwidth_integer> | <p>Enter the Kbit/sec limit for outgoing (egress) traffic for this interface.</p> <p>Use this command to configure outbound traffic shaping for an interface. Outbound traffic shaping limits the bandwidth accepted by the interface. Limiting outbound traffic takes precedence over traffic shaping applied by firewall policies.</p> <p>You can set outbound traffic shaping for any FortiGate interface and it can be active for more than one FortiGate interface at a time.</p> <p>Setting <bandwidth_integer> to 0 (the default) means unlimited bandwidth or no traffic shaping.</p> <p>This does not affect traffic offloaded to NP2, NP4 and SP3 processors.</p> | 0 |
| padt-retry-timeout <padt_retry_seconds> | <p>Initial PPPoE Active Discovery Terminate (PADT) timeout in seconds. Use this timeout to shut down the PPPoE session if it is idle for this number of seconds. PADT must be supported by your ISP.</p> <p>This is available in NAT/Route mode when mode is pppoe.</p> | 1 |
| password <pppoe_password> | <p>Enter the password to connect to the PPPoE server.</p> <p>This is available in NAT/Route mode when mode is pppoe.</p> | No default. |
| pbx-user-portal {enable disable} | <p>Enable PBX user portal on the interface.</p> <p>This command is available only on FortiGate Voice units.</p> | disable |
| phone-auto-provision {enable disable} | <p>Enable SIP phone auto-provisioning on the interface.</p> <p>This command is available only on FortiGate Voice units.</p> | disable |
| poe {disable enable} | <p>Enable or disable PoE (Power over Ethernet). This option is only available on models with PoE feature.</p> | disable |
| polling-interval <interval_int> | <p>Set the amount of time in seconds that the sFlow agent waits between sending collected data to the sFlow collector. The range is 1 to 255 seconds.</p> <p>A higher polling-interval means less data is sent across the network but also means that the sFlow collector's picture of the network may be out of date.</p> | 20 |
| pppoe-unnumbered-negotiate {disable enable} | <p>Disable to resolve problems when mode is set to PPPoE, and ipunnumbered is set. The default configuration may not work in some regions, such as Japan.</p> <p>This is only available when mode is pppoe and ipunnumbered is set.</p> | enable |

| Variable | Description | Default |
|--|---|-------------|
| pptp-client {disable enable} | Enable to configure and use a point-to-point tunneling protocol (PPTP) client. You may need to enable <code>l2forward</code> on this interface. This command is not available when in HA mode. If the pptp-client is enabled on an interface, the FortiGate unit will not enter HA mode until that pptp-client is disabled. | disable |
| pptp-user <pptp_username> | Enter the name of the PPTP user. | No default. |
| pptp-password <pptp_userpassword> | Enter the password for the PPTP user. | No default. |
| pptp-server-ip <pptp_serverid> | Enter the IP address for the PPTP server. | No default. |
| pptp-auth-type <pptp_authtype> | Enter the authentication type for the PPTP user. | No default. |
| pptp-timeout <pptp_idletimeout> | Enter the idle timeout in minutes. Use this timeout to shut down the PPTP user session if it is idle for this number of seconds. 0 for disabled. | No default. |
| priority <learned_priority> | Enter the priority of routes using this interface. For more information on priority, see “router static” on page 446 . This is only available when <code>mode</code> is <code>pppoe</code> or <code>dhcp</code> . | 0 |
| remote-ip <ipv4> | Enter an IP address for the remote end of a tunnel interface. If you want to use dynamic routing with the tunnel, or be able to ping the tunnel interface, you must specify an address for the remote end of the tunnel in <code>remote-ip</code> and an address for this end of the tunnel in <code>ip</code> . This is only available if <code>type</code> is <code>tunnel</code> . | No default. |
| replacemsg-override-group {group-name} | Enter the replacement message override group name. This is for captive portal messages when <code>security-mode</code> is <code>captive-portal</code> . | No default. |
| sample-direction {both rx tx} | Configure the sFlow agent to sample traffic received by the interface (<code>rx</code>) or sent from the interface (<code>tx</code>) or both. | both |

| Variable | Description | Default |
|--|--|---------|
| sample-rate <rate_int> | <p>Set the sample rate for the sFlow agent added to this interface. The sample rate defines the average number of packets to wait between samples. For example, the default <code>sample-rate</code> of 2000 samples 1 of every 2000 packets. The <code>sample-rate</code> range is 10 to 99999 packets between samples.</p> <p>The lower the <code>sample-rate</code> the higher the number of packets sampled. Sampling more packets increases the accuracy of the sampling data but also increases the CPU and network bandwidth required to support sFlow. The default <code>sample-rate</code> of 2000 provides high enough accuracy in most cases.</p> <p>You can increase the <code>sample-rate</code> to reduce accuracy. You can also reduce the <code>sample-rate</code> to increase accuracy.</p> | 2000 |
| secondary-IP {enable disable} | <p>Enable to add a secondary IP address to the interface. This option must be enabled before configuring a secondary IP address.</p> <p>When disabled, the web-based manager interface displays only the option to enable secondary IP.</p> | disable |
| security-groups [group1 [group2 ... groupn]] | Optionally, enter the groups that are allowed access to this interface. This is available when <code>security-mode</code> is <code>captive-portal</code> . | Null |
| security-mode {none captive-portal 802.1X} | <p>Set security mode for this interface:</p> <p>none</p> <p>captive-portal — allow only authenticated members of <code>security-groups</code> access through this interface.</p> <p>802.1X — available only on FGT60C, FWF60C, FWF60CM, FGT80C, FGT80CM, FWF80CM, FWF81C, FGT110C, and FGT111C.</p> | none |
| sflow-sampler {disable enable} | <p>Add an sFlow agent to an interface. You can also configure the sFlow agent's <code>sample-rate</code>, <code>polling-interval</code>, and <code>sample-direction</code>. You can add sFlow agents to any FortiGate interface, including physical interfaces, VLAN interfaces, and aggregate interfaces.</p> <p>After adding the sFlow agent you can configure the sFlow</p> <p>For more information about sFlow see “system sflow” on page 678.</p> | disable |
| snmp-index <id_int> | Optionally, specify the index number of this interface for SNMP purposes. | null |

| Variable | Description | Default |
|--|--|------------------------|
| speed <interface_speed> | <p>The interface speed:</p> <p>auto — the default speed. The interface uses auto-negotiation to determine the connection speed. Change the speed only if the interface is connected to a device that does not support auto-negotiation.</p> <p>10full — 10 Mbps, full duplex</p> <p>10half — 10 Mbps, half duplex</p> <p>100full — 100 Mbps, full duplex</p> <p>100half — 100 Mbps, half duplex</p> <p>1000full — 1000 Mbps, full duplex</p> <p>1000half — 1000 Mbps, half duplex</p> <p>Speed options vary for different models and interfaces. Enter a space and a “?” after the <code>speed</code> field to display a list of speeds available for your model and interface.</p> <p>You cannot change the speed for switch interfaces.</p> <p>Note: XG2 interfaces on models 3140B and 3950B cannot be configured for 1000Mbps.</p> | auto |
| spillover-threshold <threshold_int> | <p>Set the <code>spillover-threshold</code> to limit the amount of bandwidth processed by the Interface. The range is 0-16 776 000 Kbps.</p> <p>Set the spillover-threshold for an interface if the ECMP route failover and load balance method, configured by the <code>v4-ecmp-mode</code> field of the <code>config system settings</code> command is set to <code>usage-based</code>.</p> <p>The FortiGate unit sends all ECMP-routed sessions to the lowest numbered interface until the bandwidth being processed by this interface reaches its spillover threshold. The FortiGate unit then spills additional sessions over to the next lowest numbered interface.</p> | 0 |
| status {down up} | <p>Start or stop the interface. If the interface is stopped, it does not accept or send packets.</p> <p>If you stop a physical interface, associated virtual interfaces such as VLAN interfaces will also stop.</p> | up (down for VLANs) |
| stpforward {enable disable} | <p>Enable to forward Spanning Tree Protocol (STP) packets through this interface. STP maps the network to provide the least-cost-path from point to point while blocking all other ports for that path. This prevents any loops which would flood the network.</p> <p>If your network uses layer-2 protocols, and has looping issues STP will stop this. For more information, see FortiGate VLANs and VDOMs.</p> | disable |

| Variable | Description | Default |
|---|---|---|
| stpforward-mode {rpl-all-ext-id rpl-bridge-ext-id rpl-nothing} | Choose the STP forwarding mode; rpl-all-ext-id Replace all extension IDs (root, bridge). rpl-bridge-ext-id Replace bridge extension ID only. rpl-nothing Replace nothing. | rpl-all-ext-id |
| subst {enable disable} | Enable to use a substitute destination MAC address for this address. This feature may be used with virtual interfaces to prevent network loops. | disable |
| substitute-dst-mac <destination_mac_addresses> | Enter the substitute destination MAC address to use when subst is enabled. Use the xx:xx:xx:xx:xx:xx format. | No default. |
| tcp-mss <max_send_bytes> | Enter the FortiGate unit's maximum sending size for TCP packets. | No default. |
| trust-ip-1 <ipmask> trust-ip-2 <ipmask> trust-ip-3 <ipmask> | Enter trusted source addresses for this management interface. Packets from other source addresses are dropped. This is available on "mgmt" interfaces where dedicate-to is management. | 0.0.0.0/24 |
| type {aggregate hard-switch hdlc loopback physical redundant tunnel vap-switch vdom-link vlan wireless} | Enter the type of interface. Note: Some types are read only, and are set automatically by hardware. aggregate — available only on some FortiGate models. Aggregate links use the 802.3ad standard to group up to 8 interfaces together. For aggregate specific fields, see “variables for aggregate and redundant interfaces (some FortiGate models)” on page 578 . hard-switch — used when a switch-interface is configured and unit electronics provides switch functionality. The switch-interface type field must be set to switch-hardware . For more information see “switch-interface” on page 693 . hdlc — High-level Data Link Control (HDLC) is a bit-oriented synchronous data link layer protocol; it operates at Layer-2 of OSI model. It is an interface that supports T1/E1 connections. This type of interface is supported by some AMC cards. loopback — a virtual interface that is always up. This interface's status and link status are not affected by external changes. It is primarily used for blackhole routing - dropping all packets that match this route. This route is advertised to neighbors through dynamic routing protocols as any other static route. loopback interfaces have no dhcp settings, no forwarding, no mode, or dns settings. You can create a loopback interface from the CLI or web-based manager. | vlan for newly created interface, physical otherwise. |

| Variable | Description | Default |
|---|--|---|
| type {aggregate hard-switch hdlc loopback physical redundant tunnel vap-switch vdom-link vlan wireless} | <p>physical — for reference only. All physical FortiGate interfaces and only these interfaces have <code>type</code> set to <code>physical</code> and the type cannot be changed.</p> <p>redundant — used to group 2 or more interfaces together for reliability. Only one interface is in use at any given time. If the first interface fails, traffic continues uninterrupted as it switches to the next interface in the group. This is useful in HA configurations. The order interfaces become active in the group is determined by the order you specify using the <code>set member</code> field.</p> <p><code>tunnel</code> is for reference only - you cannot create tunnel interfaces using this command. Create GRE tunnels using the system gre-tunnel command. Create IPsec tunnels using the <code>vpn ipsec-intf phase1</code> command.</p> <p>vap-switch — for a wireless controller virtual access point (VAP). This type of interface is created automatically when you configure a VAP.</p> <p>vdom-link — an internal point-to-point interface object. This interface object is a link used to join virtual domains. For more information on vdom-links, see “vdom-link” on page 697.</p> <p>vlan — a virtual LAN interface. This is the type of interface created by default on any existing physical interface. VLANs increase the number of network interfaces beyond the physical connections on the unit. VLANs cannot be configured on a switch mode interface in Transparent mode.</p> <p>wireless — applies only to FortiWiFi models.</p> | vlan for newly created interface, physical otherwise. |
| username <pppoe_username> | <p>Enter the user name used to connect to the PPPoE server.</p> <p>This is only available in NAT/Route mode when <code>mode</code> is set to <code>pppoe</code>.</p> | No default. |
| vdom <vdom_name> | <p>Enter the name of the virtual domain to which this interface belongs.</p> <p>When you change this field, the physical interface moves to the specified virtual domain. Virtual IP previously added for this interface are deleted. You should also manually delete any routes that include this interface as they may now be inaccessible.</p> | root |
| vlanforward {enable disable} | Enable or disable forwarding of traffic between VLANs on this interface. When disabled, VLAN traffic will be delivered to its own VLAN only.. | enable disable (v5.0.10 and later) |

| Variable | Description | Default |
|---|---|-------------|
| vlanid <id_number> | <p>Enter a VLAN ID that matches the VLAN ID of the packets to be received by this VLAN subinterface.</p> <p>The VLAN ID can be any number between 1 and 4094, as 0 and 4095 are reserved, but it must match the VLAN ID added by the IEEE 802.1Q-compliant router on the other end of the connection. Two VLAN subinterfaces added to the same physical interface cannot have the same VLAN ID. However, you can add two or more VLAN subinterfaces with the same VLAN ID to different physical interfaces, and you can add more multiple VLANs with different VLAN IDs to the same physical interface.</p> <p>This is available only when editing an interface with a type of <code>VLAN</code>.</p> | No default. |
| voip {enable disable} | <p>Enable the VoIP SIP protocol for allowing SIP traffic on the interface.</p> <p>This command is available only on FortiGate Voice units.</p> | disable |
| vrrp-virtual-mac {enable disable} | Enable VRRP virtual MAC addresses for the VRRP routers added to this interface. See RFC 3768 for information about the VRRP virtual MAC addresses. | disable |
| wccp {enable disable} | Enable to WCCP on an interface. This setting specifies the interface the FortiGate unit sends and receives WCCP packets and redirected traffic. | disable |
| weight <int> | Set the default weight for static routes on this interface. This applies if a route has no weight configured. | 0 |
| wifi-auto-connect {enable disable} | Enable to have client mode WiFi automatically connect to nearest saved WiFi network. | enable |
| wifi-auto-save {enable disable} | Enable to have client mode WiFi automatically save the passphrase when it connects to a WiFi network. | disable |
| wins-ip <wins_server_ip> | <p>Enter the IP address of a WINS server to which to forward NetBIOS broadcasts.</p> <p>This WINS server address is only used if <code>netbios-forward</code> is enabled.</p> <p>This variable is only available in NAT/Route mode.</p> | No default. |
| config ipv6 variables | | |
| autoconf {enable disable} | <p>Enable or disable automatic configuration of the IPv6 address.</p> <p>When enabled, and <code>ip6-send-adv</code> is disabled, the FortiGate unit acts as a stateless address auto-configuration client (SLAAC).</p> | disable |
| dhcp6-relay-server {enable disable} | Enable or disable DHCP relay service for IPv6. | disable |
| dhcp6-relay-ip {ip1_ipv6 ... ipn_ipv6} | Enter the IP address of one or more IPv6 DHCP relays. This is available if <code>dhcp-relay-server</code> is enabled. | No default. |

| Variable | Description | Default |
|--|---|----------------------------|
| ip6-address <if_ipv6mask> | The interface IPv6 address and netmask. The format for IPv6 addresses and netmasks is described in RFC 3513. This is available in NAT/Route mode only. | ::/0 |
| ip6-allowaccess <access_types> | Enter the types of management access permitted on this IPv6 interface. Valid types are: fgfm, http, https, ping, snmp, ssh, and telnet. Separate the types with spaces. If you want to add or remove an option from the list, retype the list as required. | Varies for each interface. |
| ip6-default-life <ipv6_life_seconds> | Enter the number, in seconds, to add to the Router Lifetime field of router advertisements sent from the interface. The valid range is 0 to 9000. This is available in NAT/Route mode only. | 1800 |
| ip6-hop-limit <ipv6_hops_limit> | Enter the number to be added to the Cur Hop Limit field in the router advertisements sent out this interface. Entering 0 means no hop limit is specified. This is available in NAT/Route mode only. This is available in NAT/Route mode only. | 0 |
| ip6-link-mtu <ipv6_mtu> | Enter the MTU number to add to the router advertisements options field. Entering 0 means that no MTU options are sent. This is available in NAT/Route mode only. | 0 |
| ip6-manage-flag {disable enable} | Enable or disable the managed address configuration flag in router advertisements. This is available in NAT/Route mode only. | disable |
| ip6-max-interval <adverts_max_seconds> > | Enter the maximum time interval, in seconds, between sending unsolicited multicast router advertisements from the interface. The valid range is 4 to 1800. This is available in NAT/Route mode only. | 600 |
| ip6-min-interval <adverts_min_seconds> > | Enter the minimum time interval, in seconds, between sending unsolicited multicast router advertisements from the interface. The valid range is 4 to 1800. This is available in NAT/Route mode only. | 198 |
| ip6-mode {static dhcp6 pppoe} | Select either static, DHCP or PPPoE-assigned address for this interface in IPv6 operation. PPPoE is available only if IPv4 mode is pppoe. | static |
| ip6-other-flag {enable disable} | Enable or disable the other stateful configuration flag in router advertisements. This is available in NAT/Route mode only. | disable |
| ip6-reachable-time <reachable_msecs> | Enter the number to be added to the reachable time field in the router advertisements. The valid range is 0 to 3600. Entering 0 means no reachable time is specified. This is available in NAT/Route mode only. | 0 |

| Variable | Description | Default |
|---|---|---------|
| ip6-retrans-time <retrans_msecs> | Enter the number to be added to the Retrans Timer field in the router advertisements. Entering 0 means that the Retrans Timer is not specified. This is available in NAT/Route mode only. | 0 |
| ip6-send-adv {enable disable} | Enable or disable the flag indicating whether or not to send periodic router advertisements and to respond to router solicitations. When enabled, this interface's address will be added to all-routers group (FF02::02) and be included in an Multi Listener Discovery (MLD) report. If no interfaces on the FortiGate unit have ip6-send-adv enabled, the FortiGate unit will only listen to the all-hosts group (FF02::01) which is explicitly excluded from MLD reports according to RFC 2710 section 5. When disabled, and autoconf is enabled, the FortiGate unit acts as a stateless address auto-configuration client (SLAAC). This is available in NAT/Route mode only. | disable |
| edit <ip6_prefix> variables | | |
| autonomous-flag {enable disable} | Set the state of the autonomous flag for the IPv6 prefix. | disable |
| onlink-flag {enable disable} | Set the state of the on-link flag ("L-bit") in the IPv6 prefix. | |
| preferred-life-time <seconds> | Enter the preferred lifetime, in seconds, for this IPv6 prefix. | 604800 |
| valid-life-time <seconds> | Enter the valid lifetime, in seconds, for this IPv6 prefix. | 2592000 |
| config ip6-extra-addr | Configure a secondary address for this IPv6 interface. | |
| <prefix_ip6> | IPv6 address prefix. | |
| config l2tp-client-settings | | |
| auth-type {auto chap mschapv1 mschapv2 pap} | Select the type of authorization used with this client: auto — automatically choose type of authorization. chap — use Challenge-Handshake Authentication Protocol. mschapv1 — use Microsoft version of CHAP version 1. mschapv2 — use Microsoft version of CHAP version 2. pap — use Password Authentication Protocol. | auto |
| defaultgw {enable disable} | Enable to use the default gateway. | disable |
| distance <admin_distance> | Enter the administration distance of learned routes. | 2 |
| mtu <integer> | Enter the Maximum Transmission Unit (MTU) for L2TP. | 1460 |
| password <password> | Enter the password for L2TP. | n/a |

| Variable | Description | Default |
|---|--|-----------------|
| peer-host <ipv4_addr> | Enter the IP address of the L2TP host. | n/a |
| peer-mask <netmask> | Enter the netmask used to connect to L2TP peers connected to this interface. | 255.255.255.255 |
| peer-port <port_num> | Enter the port used to connect to L2TP peers on this interface. | 1701 |
| priority <integer> | Enter the priority of routes learned through L2TP. This will be used to resolve any ties in the routing table. | 0 |
| user <string> | Enter the L2TP user name used to connect. | n/a |
| variables for ADSL interface (some FortiGate models) | | |
| gwaddr <IPv4> | Enter the IP address of the gateway for this interface. | |
| mux-type {llc-encaps vc-encaps} | Enter the MUX type as either <code>llc-encaps</code> or <code>vc-encaps</code> . This information is provided by your ISP | |
| vci <integer> | Enter the virtual circuit identification VCI number. Valid numbers are from 0 to 255. This number is provided by your ISP. | 0 |
| vpi <integer> | Enter the virtual circuit identification VPI number. Valid numbers are from 0 to 65535. This number is provided by your ISP. | 35 |
| variables for aggregate and redundant interfaces (some FortiGate models) | | |
| These variables are available only when <code>type</code> is <code>aggregate</code> or <code>redundant</code> . | | |
| algorithm {L2 L3 L4} | Enter the algorithm used to control how frames are distributed across links in an aggregated interface (also called a Link Aggregation Group (LAG)). The algorithm must match that used by connected switches. Enter one of: L2 — use source and destination MAC addresses. L3 — use source and destination IP addresses, fall back to L2 algorithm if IP information is not available. L4 — use TCP, UDP or ESP header information. | L4 |
| lacp-ha-slave {enable disable} | This option affects how the aggregate interface participates in Link Aggregation Control Protocol (LACP) negotiation when HA is enabled for the VDOM. It takes effect only if Active-Passive HA is enabled and <code>lacp-mode</code> is not <code>static</code> . Enter <code>enable</code> to participate in LACP negotiation as a <code>slave</code> or <code>disable</code> to not participate. | enable |
| lacp-mode {active passive static} | Enter one of <code>active</code> , <code>passive</code> , or <code>static</code> . active — send LACP PDU packets to negotiate link aggregation connections. This is the default. passive — respond to LACP PDU packets and negotiate link aggregation connections static — link aggregation is configured statically | active |

| Variable | Description | Default |
|-------------------------------------|--|-------------|
| lacp-speed {fast slow} | <p>slow — sends LACP PDU packets every 30 seconds to negotiate link aggregation connections. This is the default.</p> <p>fast — sends LACP PDU packets every second, as recommended in the IEEE 802.3ad standard.</p> <p>This is available only when <code>type</code> is <code>aggregate</code>.</p> | slow |
| member <if_name1> <if_name2> ... | <p>Specify a list of physical interfaces that are part of an aggregate or redundant group. To modify a list, enter the complete revised list.</p> <p>If VDOMs are enabled, then <code>vdom</code> must be set the same for each interface before you enter the <code>member</code> list.</p> <p>An interface is available to be part of an aggregate or redundant group only if</p> <ul style="list-style-type: none"> • it is a physical interface, not a VLAN interface • it is not already part of an aggregated or redundant interface • it is in the same VDOM as the aggregated interface • it has no defined IP address and is not configured for DHCP or PPPoE • it has no DHCP server or relay configured on it • it does not have any VLAN subinterfaces • it is not referenced in any firewall policy, VIP or multicast policy • it is not an HA heartbeat device or monitored by HA • In a redundant group, failover to the next member interface happens when the active interface fails or is disconnected. <p>The order you specify the interfaces in the <code>member</code> list is the order they will become active in the redundant group. For example if you enter <code>set member port5 port1</code>, then <code>port5</code> will be active at the start, and when it fails or is disconnected <code>port1</code> will become active.</p> <p>This is only available when <code>type</code> is <code>aggregate</code> or <code>redundant</code>.</p> | No default. |
| VRRP fields | Add one or more VRRP virtual routers to a FortiGate interface. For information about VRRP, see RFC 3768 . | |
| <VRID_int> | VRRP virtual router ID (1 to 255). Identifies the VRRP virtual router. | |
| adv-interval <seconds_int> | VRRP advertisement interval (1-255 seconds). | 1 |
| preempt {enable disable} | Enable or disable VRRP preempt mode. In preempt mode a higher priority backup unit can preempt a lower priority master unit. | enable |

| Variable | Description | Default |
|---|---|-------------|
| priority <prio_int> | Priority of this virtual router (1-255). The VRRP virtual router on a network with the highest priority becomes the master. | 100 |
| start-time <seconds_int> | The startup time of this virtual router (1-255 seconds). The startup time is the maximum time that the backup unit waits between receiving advertisement messages from the master unit. | 3 |
| status { enable disable } | Enable or disable this virtual router. | enable |
| vrdst <ipv4_addr> | Monitor the route to this destination. | 0.0.0.0 |
| vrrip <ipv4_addr> | IP address of the virtual router. | 0.0.0.0 |
| WiFi fields (AP-mode) | | |
| mac <mac_address> | Enter a MAC address for the MAC filter list. This is used in the <code>config wifi-mac_list</code> subcommand. | No default. |
| wifi-acl { allow deny } | Select whether MAC filter list allows or denies access. | deny |
| wifi-auth { PSK radius usergroup } | Select either Pre-shared Key (PSK) or radius to authenticate users connecting to this interface. This is available only when <code>wifi-security</code> is set to WPA. Select usergroup to add a usergroup with the <code>wifi-usergroup</code> keyword. This option is only available when <code>wifi-security</code> is set to <code>wpa-enterprise</code> or <code>wpa2-enterprise</code> . | PSK |
| wifi-broadcast_ssid { enable disable } | Enable if you want FortiWiFi-60 to broadcast its SSID. | disable |
| wifi-encrypt { AES TKIP } | Select either Advanced Encryption Standard (AES) or Temporal Key Integrity Protocol (TKIP) for encryption on this WLAN interface. This is available only when <code>wifi-security</code> is set to WPA. | TKIP |
| wifi-fragment_threshold <packet_size> | Set the maximum size of a data packet before it is broken into smaller packets, reducing the chance of packet collisions. If the packet size is larger than the threshold, the FortiWiFi unit will fragment the transmission. If the packet size less than the threshold, the FortiWiFi unit will not fragment the transmission. Range 800-2346. A setting of 2346 bytes effectively disables this option. This is available in AP mode only. | 2346 |
| wifi-key <hex_key> | Enter a WEP key. The WEP key must be 10 or 26 hexadecimal digits (0-9 a-f). For a 64-bit WEP key, enter 10 hexadecimal digits. For a 128-bit WEP key, enter 26 hexadecimal digits. <code>wifi-security</code> must be set to <code>WEP128</code> or <code>WEP64</code> . This is available in AP mode only. | No default. |
| wifi-mac-filter { enable disable } | Enable MAC filtering for the wireless interface. | disable |

| Variable | Description | Default |
|-------------------------------------|---|--------------|
| wifi-passphrase <pass_str> | Enter shared key for WPA_PSK security. wifi-security must be set to WPA_PSK. This is available in AP mode only. | fortinet |
| wifi-radius-server <server_name> | Set RADIUS server name for WPA_RADIUS security. wifi-security must be set to WPA_RADIUS. This is available in AP mode only. | No default. |
| wifi-rts_threshold <integer> | The request to send (RTS) threshold is the maximum size, in bytes, of a packet that the FortiWiFi will accept without sending RTS/CTS packets to the sending wireless device. In some cases, larger packets being sent may cause collisions, slowing data transmissions. The valid range is 256 to 2346. A setting of 2347 bytes effectively disables this option. This is available in AP mode only. | 2346 |
| wifi-security <sec_mode> | Enter security (encryption) mode: none — Communication is not encrypted. wep64 — WEP 64-bit encryption wep128 — WEP 128-bit encryption wpa-personal — WPA or WPA2, personal authentication (PSK) wpa-enterprise — WPA or WPA2, enterprise authentication (802.1x) wpa2-personal — WPA2 encryption, personal authentication (PSK) wpa2-enterprise — WPA or WPA2, enterprise authentication (802.1x) wpa_radius — WPA encryption via RADIUS server. This is available in AP mode only. | wpa-personal |
| wifi-ssid <id_str> | Change the Service Set ID (SSID) as required. The SSID is the wireless network name that this FortiWiFi-60A WLAN broadcasts. Users who wish to use the wireless network should configure their computers to connect to the network that broadcasts this network name. | fortinet |
| WiFi-Networks field (Client mode) | | |
| <network_id> | Enter an integer ID. | |
| wifi-key <key_str> | Enter the pre-shared key for WEP security on this network. | No default. |
| wifi-keyindex <index_int> | Enter the pre-shared key index for WEP security on this network. | 1 |
| wifi-passphrase <psk_str> | Enter the pre-shared key for WPA-Personal security on this network. | No default. |

| Variable | Description | Default |
|---|---|--------------|
| wifi-security { wpa-personal wep128 wep64 open } | Select the security that this network uses. | wpa-personal |
| wifi-ssid <ssid_str> | Enter the SSID for this network. | fortinet |

ipip-tunnel

Use this command to set up an RFC 1853 IP-to-IP tunnel.

Syntax

```
config system ipip-tunnel
  edit <tunnel_name>
    set interface <if_name>
    set local-gw <ip4_addr>
    set remote-gw <ip4_addr>
  end
```

| Variable | Description | Default |
|----------------------|---------------------------------------|---------|
| <tunnel_name> | Enter a name for the IP-to-IP tunnel. | |
| interface <if_name> | Enter the interface to use. | |
| local-gw <ip4_addr> | Enter the local gateway IP address. | 0.0.0.0 |
| remote-gw <ip4_addr> | Enter the remote gateway IP address. | 0.0.0.0 |

ips-urlfilter-dns

Use this command to configure IPS URL filter DNS servers.

Syntax

```
config system ips-urlfilter-dns
  edit <DNS_IP>
    set status {enable | disable}
  next
end
```

| Variable | Description | Default |
|---------------------------|---------------------------------------|---------|
| <DNS_IP> | Enter the DNS server IP address. | |
| status {enable disable} | Enable or disable use of this server. | enable |

ipv6-neighbor-cache

Use this command to save neighbor cache entries for the VDOM.

Syntax

```
config system ipv6-neighbor-cache
edit <id>
    set interface <intf_name>
    set ipv6 <ipv6_addr>
    set mac <mac_addr>
end
```

| Variable | Description | Default |
|-----------------------|------------------------------|-------------------|
| interface <intf_name> | Enter the network interface. | nul |
| ipv6 <ipv6_addr> | Enter the IPv6 IP address. | :: |
| mac <mac_addr> | Enter the MAC address. | 00:00:00:00:00:00 |

ipv6-tunnel

Use this command to tunnel IPv4 traffic over an IPv6 network. The IPv6 interface is configured under `config system interface`. All subnets between the source and destination addresses must support IPv6.



This command is not available in Transparent mode.

Syntax

```
config system ipv6-tunnel
  edit <tunnel_name>
    set destination <remote_IPv6_address>
    set interface <name>
    set source <local_IPv6_address>
  end
```

| Variable | Description | Default |
|--------------------------------------|---|-------------|
| edit <tunnel_name> | Enter a name for the IPv6 tunnel. | No default. |
| destination <remote_IPv6_address> | The destination IPv6 address for this tunnel. | 0.0.0.0 |
| interface <name> | The interface used to send and receive traffic for this tunnel. | No default. |
| source <local_IPv6_address> | The source IPv6 address for this tunnel. | 0.0.0.0 |

mac-address-table

Use this command to create a static MAC table. The table can hold up to 200 entries.
This command is available in Transparent mode only.

Syntax

```
config system mac-address-table
  edit <mac-address_hex>
    set interface <if_name>
    set reply-substitute <mac-address_hex>
  end
```

| Variable | Description | Default |
|------------------------------------|--|-------------|
| edit <mac-address_hex> | Enter the MAC address as six pairs of hexadecimal digits separated by colons, e.g.: 11:22:33:00:ff:aa | No default. |
| interface <if_name> | Enter the name of the interface to which this MAC table entry applies. | No default. |
| reply-substitute <mac-address_hex> | Optionally, define a substitute MAC address to use in reply. Then define a MAC address table entry for the reply-substitute MAC address, specifying the interface to which it applies. | No default. |

modem

Use this command to configure FortiGate models with dedicated modem interfaces or to configure a serial modem interface connected using a serial converter to the USB port.

This command is only available in NAT/Route mode. When Transparent mode is enabled, all modem related pages are hidden in the web-based manager.

Syntax

```
config system modem
    set account-relation {equal | fallback}
    set altmode {enable | disable}
    set authtype1 {pap chap mschap mschapv2}
    set authtype2 {pap chap mschap mschapv2}
    set authtype3 {pap chap mschap mschapv2}
    set auto-dial {enable | disable}
    set connect_timeout <seconds>
    set dial-on-demand {enable | disable}
    set distance <distance>
    set extra-init1, extra-init2, extra-init3 <init_str>
    set holddown-timer <seconds>
    set idle-timer <minutes>
    set interface <name>
    set lockdown-lac <lac_str>
    set mode {redundant | standalone}
    set modem-dev1, modem-dev2, modem-dev3 {internal | pcmcia-
        wireless}
    set network-init <init_str>
    set passwd1, passwd2, passwd3 <password_str>
    set peer_modem1 {actiontec | ascendTNT | generic}
    set peer_modem2 {actiontec | ascendTNT | generic}
    set peer_modem3 {actiontec | ascendTNT | generic}
    set phone1 <phone-number>
    set phone2 <phone-number>
    set phone3 <phone-number>
    set pin-init <init_str>
    set ppp-echo-request1 {disable | enable}
    set ppp-echo-request2 {disable | enable}
    set ppp-echo-request3 {enable | disable}
    set priority <integer> {enable | disable}
    set redial <tries_integer>
    set status {enable | disable}
    set username1 <name_str>
    set username2 <name_str>
    set username3 <name_str>
    set wireless-port <port_int>
end
```

| Variable | Description | Default |
|---|---|--------------------------------|
| account-relation {equal fallback} | Set the account relationship as either <code>equal</code> or <code>fallback</code> . equal — Accounts are equal and keep using the first successful account. fallback — The first account takes priority, fall back to the first account if possible | equal |
| altmode {enable disable} | Enable for installations using PPP in China. | enable |
| authtype1 {pap chap mschap mschapv2} authtype2 {pap chap mschap mschapv2} authtype3 {pap chap mschap mschapv2} | Enter the authentication methods to use for 3G modems as one of: PAP, CHAP, MS-CHAP, or MS-CHAPv2. | pap chap mschap mschapv2 |
| auto-dial {enable disable} | Enable to dial the modem automatically if the connection is lost or the FortiGate unit is restarted. This is available only when <code>dial-on-demand</code> is set to <code>disabled</code> , and <code>mode</code> is set to <code>standalone</code> . | disable |
| connect_timeout <seconds> | Set the connection completion timeout (30 - 255 seconds). | 90 |
| dial-on-demand {enable disable} | Enable to dial the modem when packets are routed to the modem interface. The modem disconnects after the <code>idle-timer</code> period. This is available only if <code>auto-dial</code> is set to <code>disabled</code> , and <code>mode</code> is set to <code>standalone</code> . | disable |
| distance <distance> | Enter the administrative distance (1-255) to use for the default route that is automatically added when the modem connects and obtains an IP address. A lower distance indicates a more preferred route. For more information, see router static "distance <distance>" on page 447 . This field is useful for configuring redundant routes in which the modem interface acts as a backup to another interface. | 1 |
| extra-init1, extra-init2, extra-init3 <init_str> | Enter up to three extra initialization strings to send to the modem. | null |
| holddown-timer <seconds> | Used only when the modem is configured as a backup for an interface. Set the time (1-60 seconds) that the FortiGate unit waits before switching from the modem interface to the primary interface, after the primary interface has been restored. This is available only when <code>mode</code> is set to <code>redundant</code> . | 60 |
| idle-timer <minutes> | Set the number of minutes the modem connection can be idle before it is disconnected. This is available only if <code>mode</code> is set to <code>standalone</code> . | 5 |

| Variable | Description | Default |
|--|--|-------------|
| interface <name> | Enter an interface name to associate the modem interface with the ethernet interface that you want to either back up (backup configuration) or replace (standalone configuration). | No default. |
| lockdown-lac <lac_str> | Optionally, allow connection only to the specified location area code (LAC). | null |
| mode {redundant standalone} | Enter the required mode: redundant — The modem interface automatically takes over from a selected ethernet interface when that ethernet interface is unavailable. standalone — The modem interface is the connection from the FortiGate unit to the Internet. | standalone |
| modem-dev1, modem-dev2, modem-dev3 {internal pcmcia-wireless} | modem-dev1/2/3 refers to one of up to 3 configurable modems on your FortiGate unit. Each device can be either <i>internal</i> or <i>pcmcia-wireless</i> on models that support PCMCIA. The default is <i>internal</i> . For 3G PCMCIA modems, select the <i>pcmcia-wireless</i> option. | internal |
| network-init <init_str> | Get or set current network operator. <init_str> is equivalent to the AT command AT+COPS=<mode>,[<format>,<oper>[,<AcT>]] where <mode>: 0 — automatic selection, other parameters ignored 1 — manual selection, as specified | 0 |
| passwd1, passwd2, passwd3 <password_str> | Enter the password used to access the specified dialup account. | No default. |
| peer_modem1 {actiontec ascendTNT generic} | If the modem at phone1 is Actiontec or AscendTNT, select that type, otherwise leave setting as generic. | generic |
| peer_modem2 {actiontec ascendTNT generic} | If the modem at phone2 is Actiontec or AscendTNT, select that type, otherwise leave setting as generic. | generic |
| peer_modem3 {actiontec ascendTNT generic} | If the modem at phone3 is Actiontec or AscendTNT, select that type, otherwise leave setting as generic. | generic |
| phone1 <phone-number> phone2 <phone-number> phone3 <phone-number> | Enter the phone number required to connect to the dialup account. Do not add spaces to the phone number. Make sure to include standard special characters for pauses, country codes, and other functions as required by your modem to connect to your dialup account. | No default. |
| pin-init <init_str> | Enter an AT command string to set the PIN. Use this command only after a reboot or major settings change. | null |

| Variable | Description | Default |
|--|--|-------------|
| ppp-echo-request1 {disable enable} | Disable <code>ppp-echo-request1</code> if the PPP echo request feature is not supported by your wireless ISP. This applies to the 1st modem, if connected. PPP echo request is used to detect low level link down for modems. | enable |
| ppp-echo-request2 {disable enable} | Disable <code>ppp-echo-request2</code> if the PPP echo request feature is not supported by your wireless ISP. This applies to a 2nd modem, if connected. PPP echo request is used to detect low level link down for modems. | enable |
| ppp-echo-request3 {enable disable} | Disable <code>ppp-echo-request3</code> if the PPP echo request feature is not supported by your wireless ISP. This applies to a 3rd modem, if connected. PPP echo request is used to detect low level link down for modems. | enable |
| priority <integer> {enable disable} | Enter the priority of learned routes on this interface. Valid priorities are from 0 to 4294967295. For more information on route priorities, see “router static” on page 446 . | 0 |
| redial <tries_integer> | Set the maximum number of times (1-10) that the FortiGate unit dials the ISP to restore an active connection on the modem interface. Select <code>none</code> to allow the modem to redial without a limit. | No default. |
| status {enable disable} | Enable or disable modem support. This is equivalent to bringing an interface up or down. | disable |
| username1 <name_str> username2 <name_str> username3 <name_str> | Enter the user name used to access the specified dialup account. | No default. |
| wireless-port <port_int> | Enter TTY Port for 3G modems. Enter 0 to use default port. | 0 |

monitors

Use this command to configure top virus, top attack, policy usage and top DLP dashboard widgets.

Syntax

```
config system monitors
edit <module_id>
set widget-type <module_name>
set status {close | open}
set <custom_options>
end
```

| Variable | Description | Default |
|---|--|----------|
| <module_id> | Enter the number of this widget. Use 0 to create a new widget instance. | |
| widget-type <module_name> | Name of the system dashboard or usage widget to configure: dlp-usage — DLP archive usage widget log-monitor — Log monitor widget. pol-usage — Top Policy usage widget sessions — Top sessions dashboard widget top-attacks — Top attacks dashboard widget top-viruses — Top viruses dashboard widget | sessions |
| status {close open} | Set whether the widget is open or closed on the dashboard. | |
| <custom_options> | The custom options for the usage and dashboard widgets are listed below. | |
| Dashboard and usage widget variables | | |
| dlp-usage | Options: dlp-protocols {protocols} — enter the names of the protocols to display information for. refresh-interval <interval_int> — set the time interval for updating the widget display in the range 10 to 240 seconds or 0 to disable. report-by {dlp-rule policy profile protocol} — organize the information displayed by DLP rule name, firewall policy ID, profile name, or DLP protocol. sort-by {bytes msg-counts} — sort information by the amount of data (bytes) or the number of session (msg-counts). top-n <results_int> — set the number of results to display. The default value displays the top 10 results. | |
| log-monitor | Option: log-type {app-ctrl attack dlp event netscan spam traffic virus webfilter} — set log type to monitor | |

| Variable | Description | Default |
|-------------|--|---------|
| pol-usage | Options: display-format {chart table} — display data in a chart or a table. refresh-interval <interval_int> — set the time interval for updating the widget display in the range 10 to 240 seconds or 0 to disable. sort-by {bytes msg-counts} — sort information by the amount of data (<i>bytes</i>) or the number of session (<i>msg-counts</i>). top-n <results_int> — set the number of results to display. The default value displays the top 10 results. | |
| sessions | Options: display-format {chart table} — display data in a chart or a table. ip-version — set Internet Protocol version of sessions to display: IPv4, IPv6, or <i>ipboth</i> . refresh-interval <interval_int> — set the time interval for updating the widget display in the range 10 to 240 seconds or 0 to disable. report-by {source destination destination-port} resolve-host {enable disable} — Resolve host name. show-auth-user {enable disable} — Show authenticated user name. sort-by {bytes msg-counts} — sort information by the amount of data (<i>bytes</i>) or the number of session (<i>msg-counts</i>). top-n <results_int> — set the number of results to display. The default value displays the top 10 results. | |
| top-attacks | Options: refresh-interval <interval_int> — set the time interval for updating the widget display in the range 10 to 240 seconds or 0 to disable. top-n <results_int> — set the number of results to display. The default value displays the top 10 results. | |
| top-viruses | For the top viruses dashboard widget set the dashboard column and open and closed status and set the following options: refresh-interval <interval_int> — set the time interval for updating the widget display in the range 10 to 240 seconds or 0 to disable. top-n <results_int> — set the number of results to display. The default value displays the top 10 results. | |

nat64

Use this command to configure communication between IPv6 hosts and IPv4 servers.

Syntax

```
config system nat64
  set status {enable | disable}
  set nat64-prefix <IPv6_addr>
  set always-synthesize-aaa-record {enable | disable}
end
```

| Variable | Description | Default |
|---|---|--------------|
| status {enable disable} | Enable or disable NAT64. | disable |
| nat64-prefix <IPv6_addr> | Enter the NAT64 prefix. It must be ::/96. | 64:ff9b::/96 |
| always-synthesize-aaa-record {enable disable} | Enable or disable AAAA record synthesis. | disable |

network-visibility

Use these commands to configure network visibility settings.

Syntax

```
config system network-visibility
  set destination-hostname-visibility {enable | disable}
  set destination-location {enable | disable}
  set destination-visibility {enable | disable}
  set source-location {enable | disable}
end
```

| Variable | Description | Default |
|--|--|---------|
| destination-hostname-visibility {enable disable} | Enable or disable log destination hostname visibility | enable |
| destination-location {enable disable} | Enable or disable log destination geolocation visibility | enable |
| destination-visibility {enable disable} | Enable or disable log destination visibility | enable |
| source-location {enable disable} | Enable or disable log source geo location visibility | enable |

np6

You can use the following command to configure a wide range of settings for the NP6 processors in your FortiGate unit. You can configure different settings for each NP6 processor.

Syntax

```
config system np6
  edit <np6-processor-name>
    set fastpath {disable | enable}
    set low-latency-mode {disable | enable}
    set session-timeout-random-range <range>
    set garbage-session-collector {disable | enable}
    set session-collector-interval <range>
    set session-timeout-interval <range>
    set session-timeout-random-range <range>
    set session-timeout-fixed {disable | enable}
    config fp-anomaly-v4
      set icmp-frag {allow | drop | trap-to-host}
      set icmp-land {allow | drop | trap-to-host}
      set ipv4-land {allow | drop | trap-to-host}
      set ipv4-optlsrr {allow | drop | trap-to-host}
      set ipv4-optrr {allow | drop | trap-to-host}
      set ipv4-optsecurity {allow | drop | trap-to-host}
      set ipv4-optssrr {allow | drop | trap-to-host}
      set ipv4-optstream {allow | drop | trap-to-host}
      set ipv4-opttimestamp {allow | drop | trap-to-host}
      set ipv4-proto-err {allow | drop | trap-to-host}
      set ipv4-unknopt {allow | drop | trap-to-host}
      set tcp-land {allow | drop | trap-to-host}
      set tcp-syn-fin {allow | drop | trap-to-host}
      set tcp-winnuke {allow | drop | trap-to-host}
      set tcp_fin_noack {allow | drop | trap-to-host}
      set tcp_fin_only {allow | drop | trap-to-host}
      set tcp_no_flag {allow | drop | trap-to-host}
      set tcp_syn_data {allow | drop | trap-to-host}
      set udp-land {allow | drop | trap-to-host}
    end
    config fp-anomaly-v6
      set ipv6-daddr_err {allow | drop | trap-to-host}
      set ipv6-land {allow | drop | trap-to-host}
      set ipv6-optendpid {allow | drop | trap-to-host}
      set ipv6-opthomeaddr {allow | drop | trap-to-host}
      set ipv6-optinvld {allow | drop | trap-to-host}
      set ipv6-optjumbo {allow | drop | trap-to-host}
      set ipv6-optnsap {allow | drop | trap-to-host}
      set ipv6-optralert {allow | drop | trap-to-host}
      set ipv6-opttunnel {allow | drop | trap-to-host}
      set ipv6-proto-err {allow | drop | trap-to-host}
```

```

set ipv6-saddr_err {allow | drop | trap-to-host}
set ipv6-unknopt {allow | drop | trap-to-host}
end

```

| Variable | Description | Default |
|--|--|--------------|
| fastpath {disable enable} | Enable fastpath acceleration to offload sessions to the NP6 processor. You can disable fastpath if you don't want the NP6 processor to offload sessions. | enable |
| low-latency-mode {disable enable} | Enable low-latency mode. In low latency mode the integrated switch fabric is bypassed. Low latency mode requires that packet enter and exit using the same NP6 processor. This option is only available for NP6 processors that can operate in low-latency mode. | disable |
| per-session-accounting {disable enable} | Record traffic log messages for offloaded sessions. Enabling this feature reduces performance. | disable |
| garbage-session-collector {disable enable} | Enable deleting expired or garbage sessions. | disable |
| session-collector-interval <range> | Set the expired or garbage session collector time interval in seconds. The range is 1 to 100 seconds. | 8 |
| session-timeout-interval <range> | Set the timeout for inactive sessions. The range is 0 to 1000 seconds. | 40 |
| session-timeout-random-range <range> | Set the random timeout for inactive sessions. The range is 0 to 1000 seconds. | 8 |
| session-timeout-fixed {disable enable} | Force session timeouts at fixed, instead of random, intervals. | disable |
| config fp-anomaly-v4 options | | |
| fp-anomaly-v4 | Configure how the NP6 processor does IPv4 traffic anomaly protection. You can configure the NP6 processor to allow or drop the packets associated with an attack or forward the packets that are associated with the attack to FortiOS (called "trap-to-host"). Selecting "trap-to-host" turns off NP6 anomaly protection for that anomaly. If you require anomaly protection you can enable it with a DoS policy. | |
| icmp-frag {allow drop trap-to-host} | Detects Layer 3 fragmented packets that could be part of a layer 4 ICMP anomalies. | allow |
| icmp-land {allow drop trap-to-host} | Detects ICMP land anomalies.f | trap-to-host |
| ipv4-land {allow drop trap-to-host} | Detects IPv4 land anomalies. | trap-to-host |
| ipv4-optlsrr {allow drop trap-to-host} | Detects IPv4 with loose source record route option anomalies. | trap-to-host |
| ipv4-optrr {allow drop trap-to-host} | Detects IPv4 with record route option anomalies. | trap-to-host |
| ipv4-optsecurity {allow drop trap-to-host} | Detects security option anomalies. | trap-to-host |
| ipv4-optssrr {allow drop trap-to-host} | Detects IPv4 with strict source record route option anomalies. | trap-to-host |

| Variable | Description | Default |
|---|--|--------------|
| ipv4-optstream {allow drop trap-to-host} | Detects stream option anomalies. | trap-to-host |
| ipv4-opttimestamp {allow drop trap-to-host} | Detects timestamp option anomalies. | trap-to-host |
| ipv4-proto-err {allow drop trap-to-host} | Detects invalid layer 4 protocol anomalies. | trap-to-host |
| ipv4-unknopt {allow drop trap-to-host} | Detects unknown option anomalies. | trap-to-host |
| tcp-land {allow drop trap-to-host} | Detects TCP land anomalies. | trap-to-host |
| tcp-syn-fin {allow drop trap-to-host} | Detects TCP SYN flood SYN/FIN flag set anomalies. | allow |
| tcp-winnuke {allow drop trap-to-host} | Detects TCP WinNuke anomalies. | trap-to-host |
| tcp_fin_noack {allow drop trap-to-host} | Detects TCP SYN flood with FIN flag set without ACK setting anomalies. | trap-to-host |
| tcp_fin_only {allow drop trap-to-host} | Detects TCP SYN flood with only FIN flag set anomalies. | trap-to-host |
| tcp_no_flag {allow drop trap-to-host} | Detects TCP SYN flood with no flag set anomalies. | allow |
| tcp_syn_data {allow drop trap-to-host} | Detects TCP SYN flood packets with data anomalies. | allow |
| udp-land {allow drop trap-to-host} | Detects UDP land anomalies. | trap-to-host |
| config fp-anomaly-v6 options | | |
| fp-anomaly-v6 | Configure how the NP6 processor does IPv6 traffic anomaly protection. You can configure the NP6 processor to allow or drop the packets associated with an attack or forward the packets that are associated with the attack to FortiOS (called “trap-to-host”). Selecting “trap-to-host” turns off NP6 anomaly protection for that anomaly. If you require anomaly protection you can enable it with a DoS policy. | |
| ipv6-daddr_err {allow drop trap-to-host} | Detects destination address as unspecified or loopback address anomalies. | trap-to-host |
| ipv6-land {allow drop trap-to-host} | Detects IPv6 land anomalies. | trap-to-host |
| ipv6-optendpid {allow drop trap-to-host} | Detects end point identification anomalies. | trap-to-host |
| ipv6-opthomeaddr {allow drop trap-to-host} | Detects home address option anomalies. | trap-to-host |
| ipv6-optinvld {allow drop trap-to-host} | Detects invalid option anomalies. | trap-to-host |
| ipv6-optjumbo {allow drop trap-to-host} | Detects jumbo options anomalies. | trap-to-host |
| ipv6-optnsap {allow drop trap-to-host} | Detects network service access point address option anomalies. | trap-to-host |

| Variable | Description | Default |
|--|--|--------------|
| ipv6-optralert {allow drop trap-to-host} | Detects router alert option anomalies. | trap-to-host |
| ipv6-opttunnel {allow drop trap-to-host} | Detects tunnel encapsulation limit option anomalies. | trap-to-host |
| ipv6-proto-err {allow drop trap-to-host} | Detects layer 4 invalid protocol anomalies. | trap-to-host |
| ipv6-saddr_err {allow drop trap-to-host} | Detects source address as multicast anomalies. | trap-to-host |
| ipv6-unknopt {allow drop trap-to-host} | Detects unknown option anomalies. | trap-to-host |

npu

Use this command to configure the Network Processing Unit (NPU) for FortiGate units that support FB4. The NPU can take over encryption processing for its interfaces that would normally be performed by the main FortiGate unit CPU.



If you use the `traffic-shaping-mode` command, the `bidirection` option counts twice as much traffic. You need to allow twice the bandwidth as with `unidirection`.

Syntax

```
config system npu
    set dec-offload-antireplay {enable | disable}
    set dedicated-management-cpu {enable | disable}
    set dedicated-tx-npu {enable | disable}
    set enc-offload-antireplay {enable | disable}
    set npu-cascade-cluster {enable | disable}
    set offload-ipsec-host {enable | disable}
next
end
```

| Variable | Description | Default |
|--|---|---------|
| dec-offload-antireplay {enable disable} | Enable this option for the system to offload IPSEC packet encryption to FB4 when the ingress port of the tunnel is on FB4. | enable |
| dedicated-management-cpu {enable disable} | Enable dedicating CPU #0 to management functions. This can affect performance. Available on some models. | disable |
| dedicated-tx-npu {enable disable} | Enable a special mode in NP4, which handles slow path packets using a dedicated third NP4. This is available on model 3600C only. | disable |
| enc-offload-antireplay {enable disable} | Enable this option for the system to offload IPSEC packet encryption to FB4 when the egress port of the tunnel is on FB4. | disable |
| npu-cascade-cluster {enable disable} | Enable cascade cluster mode on models 3950B and 3951B. Not available if <code>sp-load-balance</code> is enabled in <code>system global</code> . | disable |
| offload-ipsec-host {enable disable} | Enable this option for the system to offload packet encryption to FB4 when the egress port of this packet is on FB4. | disable |

ntp

Use this command to configure Network Time Protocol (NTP) servers.

Syntax

```
config system ntp
  set ntpsync {enable | disable}
  set source-ip <ipv4_addr>
  set syncinterval <interval_int>
  set type {fortiguard | custom}
  set server-mode {enable | disable}
  set interface <interface_list>
  config ntpserver
    edit <serverid_int>
      set authentication {enable | disable}
      set key <password_str>
      set key-id <int>
      set ntpv3 {enable | disable}
      set server {<ipv4_addr> | <hostname_str> |
        <ipv4_addr>/<hostname_str>}
    end
  end
```

| Variable | Description | Default |
|--|--|-------------|
| interface <interface_list> | Enter a space-separated list of interfaces on which the NTP server is available. This is available when server-mode is enabled. | No default. |
| ntpsync {enable disable} | Enable to synchronize FortiGate unit's system time with the ntp server. | disable |
| server-mode {enable disable} | Enable or disable FortiGate unit NTP server. | disable |
| source-ip <ipv4_addr> | Enter the source IP for communications to the NTP server. | 0.0.0.0 |
| syncinterval <interval_int> | Enter the interval in minutes between contacting NTP server to synchronize time. The range is from 1 to 1440 minutes. Only valid when ntpsync is enabled. | 0 |
| type {fortiguard custom} | Select FortiGuard or custom NTP server. | fortiguard |
| config ntpserver fields | | |
| edit <serverid_int> | Enter the number for this NTP server | |
| authentication {enable disable} | Enable or disable MD5 authentication. | disable |
| key <password_str> | Enter the password for MD5 authentication. | null |
| key-id <int> | Enter the Key-ID value for MD5 authentication. | 0 |
| ntpv3 {enable disable} | Use NTPv3 protocol instead of NTPv4. | disable |
| server {<ipv4_addr> <hostname_str> <ipv4_addr>/<hostname_str>} | Enter the IPv4 address or host name for the NTP server. You can also add an IPv4 address and hostname in the format 1.1.1.1/abcd. | |

object-tag

Use this command to configure object tags.

Syntax

```
config system object-tag
edit <tag-name>
```

| Variable | Description | Default |
|-----------------|----------------------------|-------------|
| edit <tag-name> | Enter the object tag name. | No default. |

password-policy

Use this command to configure higher security requirements for administrator passwords and IPsec VPN pre-shared keys.

Syntax

```
config system password-policy
    set status {enable | disable}
    set apply-to [admin-password ipsec-preshared-key]
    set change-4-characters {enable | disable}
    set expire <days>
    set minimum-length <chars>
    set min-lower-case-letter <num_int>
    set min-upper-case-letter <num_int>
    set min-non-alphanumeric <num_int>
    set min-number <num_int>
    set expire-status {enable | disable}
    set expire-day <num_int>
end
```

| Variable | Description | Default |
|---|--|----------------|
| apply-to [admin-password ipsec-preshared-key] | Select where the policy applies: administrator passwords or IPSec preshared keys. | admin-password |
| change-4-characters {enable disable} | Enable to require the new password to differ from the old password by at least four characters. | disable |
| expire <days> | Set time to expiry in days. Enter 0 for no expiry. | 0 |
| minimum-length <chars> | Set the minimum length of password in characters. Range 8 to 32. | 8 |
| min-lower-case-letter <num_int> | Enter the minimum number of required lower case letters in every password. | 0 |
| min-upper-case-letter <num_int> | Enter the minimum number of required upper case letters in every password. | 0 |
| min-non-alphanumeric <num_int> | Enter the minimum number of required non-alphanumeric characters in every password. | 0 |
| min-number <num_int> | Enter the minimum number of number characters required in every password. | 0 |
| expire-status {enable disable} | Enable to have passwords expire. | enable |
| expire-day <num_int> | Enter the number of days before the current password is expired and the user will be required to change their password. This option is available only when <code>expire-status</code> is set to enable. | 90 |
| status {enable disable} | Enable password policy. | disable |

physical-switch

Use this command to configure the Layer 2 functions on FortiGate unit hardware-based switches.

Syntax

```
config system physical-switch
  edit <switch_name>
    set age-enable {enable | disable}
    set age-val <int>
  end
```

| Variable | Description | Default |
|----------------------------------|---|-----------|
| <switch_name> | Select the hardware switch (sw0 for example). | |
| age-enable {enable disable} | Enable or disable Layer 2 Ageing Timer | disable |
| age-val <int> | Enter the age value. | 3 158 067 |

port-pair

Use this command to define a port pair in Transparent mode. In a port pair, all L2 packets received on one port are forwarded to the other port. It is not possible to define firewall policies into or out of the port-pair, only between the members of the pair. A maximum of 256 port pairs can be defined in any VDOM, 512 globally.

Syntax

```
config system port-pair
  edit <port-pair_name>
    set member <portname1> <portname2>
  end
```

| Variable | Description | Default |
|--------------------------------|--|-------------|
| edit <port-pair_name> | Enter a name for the port pair. | No default. |
| member <portname1> <portname2> | Enter the two port names that comprise the pair. | No default. |

probe-response

Use this command to configure probe responses.

Syntax

```
config system probe-response
  set http-probe {enable | disable}
  set http-probe-value <string>
  set mode {http-probe | twamp}
  set port <port_int>
end
```

| Variable | Description | Default |
|-------------------------------|---|------------|
| http-probe {enable disable} | Enable or disable probe response. | disable |
| http-probe-value <string> | Enter content of probe response. | OK |
| mode {http-probe twamp} | Select either HTTP-probe or Two-Way Active Measurement Protocol (TWAMP) mode. | http-probe |
| port <port_int> | Enter to port to respond on. | 8008 |

proxy-arp

Use this command to add IP addresses to MAC address translation entries to the proxy ARP table.

Syntax

```
config system proxy-arp
  edit <table_entry>
    set interface <port>
    set ip <ipv4_address>
  next
end
```

| Variable | Description | Default |
|--------------------|--|-------------|
| edit <table_entry> | Enter the unique ID of the table entry to add or modify. | No default. |
| interface <port> | Enter the physical port this IP will be associated with. | No default. |
| ip <ipv4_address> | Enter the IP address to associate with this physical port. | No default. |

pstn

Use this command to configure the PSTN interfaces. PSTN interfaces are available on some FortiGate Voice models.

Syntax

```
config system pstn
  edit <fxo_name>
    set cid-name <caller_name>
    set cid-number <caller_name>
    set status {enable | disable}
    set use-callerid {enable | disable}
    set cid-signalling {bell | dtmf | v23 | v23-jp}
    set cid-start {polarity | ring}
    set send-callerid-after <integer>
    set hangup-on-polarity-reversal {enable | disable}
    set hangup-on-zero-voltage {enable | disable}
    set hangup-on-busy-tone {enable | disable}
    set busycount <integer>
    set busy-tone-length <integer>
    set busy-quiet-length <integer>
    set codec {alaw | ulaw}
  end
```

| Variables | Description | Default |
|--|---|------------|
| edit <fxo_name> | Enter the name of the FXO. | No default |
| cid-name <caller_name> | This name is used for caller ID for calls from the FortiGate Voice unit to the PSTN. It can be any name, such as a company name, that identifies the branch office. | No default |
| cid-number <caller_name> | Enter the phone number of the PSTN phone line as provided by your phone service provider. | No default |
| status {enable disable} | Enable the status of the port. | enable |
| use-callerid {enable disable} | Enable to catch the caller ID. | enable |
| cid-signalling {bell dtmf v23 v23-jp} | Enter the caller ID protocol. The protocol v23-jp is the v23 protocol for Japan. | bell |
| cid-start {polarity ring} | Enter to start transmitting the caller ID. | ring |
| send-callerid-after <integer> | Enter a number for the number of rings after that the caller ID began to transmit. | 1 |
| hangup-on-polarity-reversal {enable disable} | Enable to have the phone hang up when there is polarity reversal. | enable |
| hangup-on-zero-voltage {enable disable} | Enable to have the phone hang up when there is zero voltage. | disable |
| hangup-on-busy-tone {enable disable} | Enable to have the phone hang up when a busy tone is detected. | enable |
| busycount <integer> | Enter a number for the accurate number of busy tones that are detected. | 4 |

| Variables | Description | Default |
|---|---|---------------|
| busy-tone-length <integer> | Enter a number that determines how long the busy tone is on in milliseconds. | 500 |
| busy-quiet-length <integer> | Enter a number that determines how long the busy tone is off in milliseconds. | 500 |
| codec {alaw ulaw} | Enter the Codec preference type based on the country. | ulaw |
| ring-detect {ring-cross-threshold ring-full-wave ring-half-wave ring-validate} | Enter the appropriate ring detection method for your phone system. | ring-validate |
| ring-timeout {128ms 256ms 384ms 512ms 640ms 768ms 896ms 1024ms 1152ms 1280ms 1408ms 1536ms 1664ms 1792ms 1920ms} | Enter the appropriate ring time-out for your phone system. | 640ms |
| ring-threshold {level-1 level-2 level-3} | Enter the appropriate ring threshold for your phone system. The ring-threshold is based on voltage: <ul style="list-style-type: none"> level-1: 13.5V to 16.5V level-2: 19.35V to 23.65V level-3: 40.5V to 49.5V | level-1 |
| ring-delay-time {256ms 512ms 768ms 1024ms 1280ms 1536ms 1792ms} | Enter the appropriate ring delay time for your phone system. | 512ms |
| ring-confirm-time {100ms 150ms 200ms 256ms 384ms 512ms 640ms 1024ms} | Enter the appropriate ring confirmation time for your phone system. | 512ms |
| ring-max-assertion-count <int> | Enter the appropriate ring maximum assertion count for your phone system. | 22 |
| ring-assertion-time <int> | Enter the appropriate ring assertion time for your phone system. | 25 |
| tx-gain <int> | Enter the gain for the transmitted signal, in dB, from -15 to 12. | 0 |
| rx-gain <int> | Enter the gain for the received signal, in dB, from -15 to 12. | 0 |

replacemsg admin

Use this command to change the administration disclaimer page.

If you enter the following CLI command the FortiGate unit displays the Administration Login disclaimer whenever an administrator logs into the FortiGate unit web-based manager or CLI.

```
config system global
    set pre-login-banner enable
    set post-login-banner enable
end
```

The web-based manager administrator login disclaimer contains the text of the Login Disclaimer replacement message as well as Accept and Decline buttons. The administrator must select accept to login.

These are HTML messages with HTTP headers.

Syntax

```
config system replacemsg admin admin_disclaimer_text
    set buffer <message>
    set format <format>
    set header <header_type>
end
```

| Variable | Description | Default |
|----------------------|---|--------------------------|
| buffer <message> | Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters. | Depends on message type. |
| format <format> | Set the format of the message: html, text, or none. | No default. |
| header <header_type> | Set the format of the message header: 8bit, http, or none. | Depends on message type. |

Replacement messages can include replacement message tags. When users receive the replacement message, the replacement message tag is replaced with content relevant to the message. Generally there is not a large call for these tags in disclaimer pages.

Table 2: Replacement message tags

| Tag | Description |
|--------------------|---|
| %%AUTH_REDIR_URL%% | Link to open a new window. (optional). |
| %%AUTH_LOGOUT%% | Immediately close the connection policy. |
| %%KEEPALIVEURL%% | URL the keep alive page connects to that keeps the connection policy alive. Connects every %%TIMEOUT%% seconds. |
| %%TIMEOUT%% | Configured number of seconds between %%KEEPALIVEURL%% connections. |

replacemsg alertmail

The FortiGate unit adds the alert mail replacement messages listed to alert email messages sent to administrators. For more information about alert email, see “[system email-server](#)” on [page 514](#).

Alert mail replacement messages are text messages.

These are HTML messages with HTTP headers.

Syntax

```
config system replacemsg alertmail alert_msg_type
    set buffer <message>
    set format <format>
    set header <header_type>
end
```

| Variable | Description | Default |
|----------------------|---|--------------------------|
| alert_msg_type | FortiGuard replacement alertmail message type. See Table 3 . | No default. |
| buffer <message> | Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters. | Depends on message type. |
| format <format> | Set the format of the message: html text none | No default. |
| header <header_type> | Set the format of the message header: 8bit http none | Depends on message type. |



If you enable *Send alert email for logs based on severity* for alert email, whether or not replacement messages are sent by alert email depends on how you set the alert email *Minimum log level*.

Table 3: alertmail message types

| Message Type | Description |
|----------------------|---|
| alertmail-block | <i>Virus detected</i> must be enabled for alert email. Antivirus <i>File Filter</i> must be enabled in an antivirus profile, and it must block a file that matches an entry in a selected file filter list. |
| alertmail-crit-event | Whenever a critical level event log message is generated, this replacement message is sent unless you configure alert email to enable <i>Send alert email for logs based on severity</i> and set the <i>Minimum log level</i> to <i>Alert</i> or <i>Emergency</i> . |

Table 3: alertmail message types

| | |
|----------------------|---|
| alertmail-disk-full | <i>Disk usage</i> must be enabled, and disk usage reaches the percent full amount configured for alert email. For more information, see “system email-server” on page 514 . |
| alertmail-nids-event | <i>Intrusion detected</i> must be enabled for alert email. When an IPS Sensor or a DoS Sensor detects an attack, this replacement message will be sent. |
| alertmail-virus | <i>Virus detected</i> must be enabled for alert email. Antivirus <i>Virus Scan</i> must be enabled in an antivirus profile and detect a virus. |

Replacement messages can include replacement message tags. When users receive the replacement message, the replacement message tag is replaced with content relevant to the message.

Table 4: Replacement message tags

| Tag | Description |
|--------------------|---|
| %%FILE%% | The name of a file that has been removed from a content stream. This could be a file that contained a virus or was blocked by antivirus file blocking. %%FILE%% can be used in virus and file block messages. |
| %%VIRUS%% | The name of a virus that was found in a file by the antivirus system. %%VIRUS%% can be used in virus messages |
| %%URL%% | The URL of a web page. This can be a web page that is blocked by web filter content or URL blocking. %%URL%% can also be used in http virus and file block messages to be the URL of the web page from which a user attempted to download a file that is blocked. |
| %%CRITICAL_EVENT%% | Added to alert email critical event email messages. %%CRITICAL_EVENT%% is replaced with the critical event message that triggered the alert email. |
| %%PROTOCOL%% | The protocol (HTTP, FTP, POP3, IMAP, SMTP) in which a virus was detected. %%PROTOCOL%% is added to alert email virus messages. |
| %%SOURCE_IP%% | IP address of the email server that sent the email containing the virus. |
| %%DEST_IP%% | IP address of the user's computer that attempted to download the message from which the file was removed. |
| %%EMAIL_FROM%% | The email address of the sender of the message from which the file was removed. |
| %%EMAIL_TO%% | The email address of the intended receiver of the message from which the file was removed. |
| %%NIDS_EVENT%% | The IPS attack message. %%NIDS_EVENT%% is added to alert email intrusion messages. |

replacemsg auth

The FortiGate unit uses the text of the authentication replacement messages listed in [Table 6](#) for various user authentication HTML pages that are displayed when a user is required to authenticate because a firewall policy includes at least one identity-based policy that requires firewall users to authenticate.

These pages are used for authentication using HTTP and HTTPS. Authentication replacement messages are HTML messages. You cannot customize the firewall authentication messages for FTP and Telnet.

The authentication login page and the authentication disclaimer include replacement tags and controls not found on other replacement messages.

Users see the authentication login page when they use a VPN or a firewall policy that requires authentication. You can customize this page in the same way as you modify other replacement messages,

Administrators see the authentication disclaimer page when logging into the FortiGate web-based manager or CLI. The disclaimer page makes a statement about usage policy to which the user must agree before the FortiGate unit permits access. You should change only the disclaimer text itself, not the HTML form code.

There are some unique requirements for these replacement messages:

- The login page must be an HTML page containing a form with ACTION="/" and METHOD="POST"
- The form must contain the following hidden controls:
 - `<INPUT TYPE="hidden" NAME="%%MAGICID%%" VALUE="%%MAGICVAL%%">`
 - `<INPUT TYPE="hidden" NAME="%%STATEID%%" VALUE="%%STATEVAL%%">`
 - `<INPUT TYPE="hidden" NAME="%%REDIRID%%" VALUE="%%PROTURI%%">`
- The form must contain the following visible controls:
 - `<INPUT TYPE="text" NAME="%%USERNAMEID%%" size=25>`
 - `<INPUT TYPE="password" NAME="%%PASSWORDID%%" size=25>`

These are HTML messages with HTTP headers.

Syntax

```
config system replacemsg auth auth_msg_type
    set buffer <message>
    set format <format>
    set header <header_type>
end
```

| Variable | Description | Default |
|------------------|---|--------------------------|
| auth_msg_type | FortiGuard replacement message type. See Table 5 on page 614 . | No default |
| buffer <message> | Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters. | Depends on message type. |

| Variable | Description | Default |
|----------------------|---|--------------------------|
| format <format> | Set the format of the message: html text none | No default |
| header <header_type> | Set the format of the message header: 8bit http none | Depends on message type. |

Table 5: auth message types

| Message Type | Description |
|------------------------|--|
| auth-challenge-page | <p>This HTML page is displayed if firewall users are required to answer a question to complete authentication. The page displays the question and includes a field in which to type the answer. This feature is supported by RADIUS and uses the generic RADIUS challenge-access auth response. Usually, challenge-access responses contain a Reply-Message attribute that contains a message for the user (for example, "Please enter new PIN"). This message is displayed on the login challenge page. The user enters a response that is sent back to the RADIUS server to be verified.</p> <p>The Login challenge page is most often used with RSA RADIUS server for RSA SecurID authentication. The login challenge appears when the server needs the user to enter a new PIN. You can customize the replacement message to ask the user for a SecurID PIN.</p> <p>This page uses the %%QUESTION%% tag.</p> |
| auth-disclaimer[1 2 3] | <p>Prompts user to accept the displayed disclaimer when leaving protected network.</p> <p>The web-based manager refers to this as <i>User Authentication Disclaimer</i>, and it is enabled with a firewall policy that also includes at least one identity-based policy. When a firewall user attempts to browse a network through the FortiGate unit using HTTP or HTTPS this disclaimer page is displayed.</p> <p>The extra pages seamlessly extend the size of the page from 8 192 characters to 16 384 and 24 576 characters respectively.</p> |

Table 5: auth message types

| | |
|------------------------------|---|
| auth-keepalive-page | <p>The HTML page displayed with firewall authentication keepalive is enabled using the following CLI command:</p> <pre>config system global set auth-keepalive enable end</pre> <p>Authentication keepalive keeps authenticated firewall sessions from ending when the authentication timeout ends. In the web-based manager, go to <i>User > Options</i> to set the <i>Authentication Timeout</i>.</p> <p>This page includes %%TIMEOUT%%.</p> |
| auth-login-failed-page | <p>The HTML page displayed if firewall users enter an incorrect user name and password combination.</p> <p>This page includes %%FAILED_MESSAGE%%, %%USERNAMEID%%, and %%PASSWORDID%% tags.</p> |
| auth-login-page | <p>The authentication HTML page displayed when firewall users who are required to authenticate connect through the FortiGate unit using HTTP or HTTPS.</p> <p>Prompts the user for their username and password to login.</p> <p>This page includes %%USERNAMEID%% and %%PASSWORDID%% tags.</p> |
| auth-reject-page | <p>The <i>Disclaimer page</i> replacement message does not re-direct the user to a redirect URL or the firewall policy does not include a redirect URL. When a firewall user selects the button on the disclaimer page to decline access through the FortiGate unit, the <i>Declined disclaimer page</i> is displayed.</p> |
| auth-token-login-page | <p>The authentication HTML page displayed when firewall users who are required to use two-factor authentication connect through the FortiGate unit using HTTP or HTTPS.</p> <p>Prompts the user for their username, password and two-factor authentication credentials.</p> <p>This page includes %%USERNAMEID%%, %%PASSWORDID%%, and %%TOKENCODE%% tags.</p> |
| auth-token-login-failed-page | <p>The HTML page displayed if firewall users performing two-factor authentication enter an incorrect credentials.</p> <p>This page includes %%USERNAMEID%%, %%PASSWORDID%%, and %%TOKENCODE%% and %%EXTRAINFO%% tags.</p> |

Replacement messages can include replacement message tags. When users receive the replacement message, the replacement message tag is replaced with content relevant to the message.

Table 6: Replacement message tags

| Tag | Description |
|--------------------|--|
| %%AUTH_REDIR_URL%% | Link to open a new window. (optional). |
| %%AUTH_LOGOUT%% | Immediately close the connection policy. |

Table 6: Replacement message tags

| Tag | Description |
|--------------------|--|
| %%EXTRAINFO%% | Provide extra help on two-factor authentication. |
| %%FAILED_MESSAGE%% | Message displayed on failed login page after user login fails. |
| %%KEEPALIVEURL%% | URL the keep alive page connects to that keeps the connection policy alive. Connects every %%TIMEOUT%% seconds. |
| %%QUESTION%% | The default login and rejected login pages use this text immediately preceding the username and password fields. The default challenge page uses this as the challenge question. These are treated as two different variables by the server. If you want to use different text, replace %%QUESTION%% with the text that you prefer. |
| %%TIMEOUT%% | Configured number of seconds between %%KEEPALIVEURL%% connections. |
| %%TOKENCODE%% | The FortiToken authentication code. Used for two-factor authentication. |
| %%USERNAMEID%% | Username of the user logging in. This tag is used on the login and failed login pages. |
| %%PASSWORDID%% | Password of the user logging in. This tag is used on the challenge, login and failed login pages. |

Requirements for login page

The authentication login page is linked to FortiGate functionality and you must construct it according to the following guidelines to ensure that it will work.

- The login page must be an HTML page containing a form with ACTION="/" and METHOD="POST"
- The form must contain the following hidden controls:
 - `<INPUT TYPE="hidden" NAME="%%MAGICID%%" VALUE="%%MAGICVAL%%">`
 - `<INPUT TYPE="hidden" NAME="%%STATEID%%" VALUE="%%STATEVAL%%">`
 - `<INPUT TYPE="hidden" NAME="%%REDIRID%%" VALUE="%%PROTURI%%">`
- The form must contain the following visible controls:
 - `<INPUT TYPE="text" NAME="%%USERNAMEID%%" size=25>`
 - `<INPUT TYPE="password" NAME="%%PASSWORDID%%" size=25>`

replacemsg device-detection-portal

The device-detection-portal messages report device detection events to the user. Currently only the device detection failure message is supported.

Syntax

```
config system replacemsg device-detection-portal device-detection-failure
    set buffer <message>
    set format <format>
    set header <header_type>
end
```

| Variable | Description | Default |
|--------------------------|---|--------------------------|
| device-detection-failure | The FortiGate unit sends this message if it cannot determine the device type. | No default |
| buffer <message> | Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters. | Depends on message type. |
| format <format> | Set the format of the message: html text none | html |
| header <header_type> | Set the format of the message header: 8bit http none | http |

replacemsg ec

The endpoint control (ec) replacement messages format the portal pages that the FortiGate unit sends to non-compliant users who attempt to use a firewall policy in which Endpoint NAC (endpoint-check) is enabled.

There are two Endpoint NAC portals:

- *Endpoint NAC Download Portal* — The FortiGate unit sends this page if the Endpoint NAC profile has `recommendation-disclaimer` disabled. In the web-based manager, this is the *Quarantine Hosts to User Portal (Enforce compliance)* option. The user can download the FortiClient Endpoint Security application installer. If you modify this replacement message, be sure to retain the `%%LINK%%` tag which provides the download URL for the FortiClient installer.
- *Endpoint NAC Recommendation Portal* — The FortiGate unit sends this page if the Endpoint NAC profile has `recommendation-disclaimer` enabled. In the web-based manager, this is the *Notify Hosts to Install FortiClient (Warn only)* option. The user can either download the FortiClient Endpoint Security application installer or select the *Continue to* link to access their desired destination. If you modify this replacement message, be sure to retain both the `%%LINK%%` tag which provides the download URL for the FortiClient installer and the `%%DST_ADDR%%` link that contains the URL that the user requested.

Message format is HTML by default.

Syntax

```
config system replacemsg ec endpt-download-portal
    set buffer <message>
    set format <format>
    set header <header_type>
end
config system replacemsg ec endpt-recommendation-portal
    set buffer <message>
    set format <format>
    set header <header_type>
end
```

| Variable | Description | Default |
|-----------------------------|---|------------|
| endpt-download-portal | The Endpoint NAC Download Portal. The FortiGate unit sends this message to non-compliant users if <code>recommendation-disclaimer</code> is disabled in the Endpoint Control profile. The user can download the FortiClient Endpoint Security application installer. | No default |
| endpt-recommendation-portal | The Endpoint NAC Recommendation Portal. The FortiGate unit sends this message to non-compliant users if <code>recommendation-disclaimer</code> is enabled in the Endpoint Control profile. The user can either download the FortiClient Endpoint Security application installer or select the <i>Continue to</i> link to access their desired destination. | No default |

| Variable | Description | Default |
|----------------------|---|--------------------------|
| buffer <message> | Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters. | Depends on message type. |
| format <format> | Set the format of the message: html text none | |
| header <header_type> | Set the format of the message header: 8bit http none | |

The endpoint control replacement messages include the following replacement message tags. When users receive the replacement message, the replacement message tag is replaced with the appropriate content.

Table 7: Replacement message tags

| Tag | Description |
|--------------|--|
| %%LINK%% | The download URL for the FortiClient installer. |
| %%DST_ADDR%% | The destination URL that the user entered. This is used in the <code>endpt-recommendation-portal</code> message only. |

replacemsg fortiguard-wf

Use this command to change the default messages that replace a web pages that FortiGuard web filtering has blocked.

The FortiGate unit sends the FortiGuard Web Filtering replacement messages listed in [Table 8](#) to web browsers using the HTTP protocol when FortiGuard web filtering blocks a URL, provides details about blocked HTTP 4xx and 5xx errors, and for FortiGuard overrides. FortiGuard Web Filtering replacement messages are HTTP pages.

If the FortiGate unit supports SSL content scanning and inspection these replacement messages can also replace web pages downloaded using the HTTPS protocol.

By default, these are HTML messages.

Syntax

```
config system replacemsg fortiguard-wf <fortiguard_msg_type>
  set buffer <message>
  set format <format>
  set header <header_type>
end
```

| Variable | Description | Default |
|-----------------------|---|--------------------------|
| <fortiguard_msg_type> | FortiGuard replacement message type. See Table 8 . | No default. |
| buffer <message> | Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters. | Depends on message type. |
| format <format> | Set the format of the message: html text none | No default |
| header <header_type> | Set the format of the message header: 8bit http none | Depends on message type. |

Table 8: FortiGuard Web Filtering replacement messages

| Message name | Description |
|--------------|--|
| ftgd-block | <i>Enable FortiGuard Web Filtering</i> is enabled in a web filter profile for HTTP or HTTPS, and blocks a web page. The blocked page is replaced with the <code>ftgd-block</code> web page. |
| ftgd-ovrd | <p>Override selected filtering for a FortiGuard Web Filtering category and FortiGuard Web Filtering blocks a web page in this category. displays this web page. Using this web page users can authenticate to get access to the page. Go to <i>UTM > Web Filter > Override</i> to add override rules. For more information, see “webfilter override” on page 862.</p> <p>The <code>%%OVRD_FORM%%</code> tag provides the form used to initiate an override if FortiGuard Web Filtering blocks access to a web page. Do not remove this tag from the replacement message.</p> |
| http-err | <i>Provide details for blocked HTTP 4xx and 5xx errors</i> is enabled in a web filter profile for HTTP or HTTPS, and blocks a web page. The blocked page is replaced with the <code>http-err</code> web page. |

replacemsg ftp

The FortiGate unit sends the FTP replacement messages to FTP clients when an event occurs such as antivirus blocking a file that contains a virus in an FTP session.

By default, these are text-format messages with no header.

Syntax

```
config system replacemsg ftp <message-type>
    set buffer <message>
    set format <format>
    set header <header_type>
end
```

| Variable | Description | Default |
|----------------------|---|--------------------------|
| <message-type> | FTP replacement message type. See Table 9 . | No default. |
| buffer <message> | Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters. | Depends on message type. |
| format <format> | Set the format of the message: html text none | No default |
| header <header_type> | Set the format of the message header: 8bit http none | Depends on message type. |

Table 9: FTP replacement messages

| Message name | Description |
|----------------------|---|
| explicit-banner | Greeting banner for explicit FTP proxy. |
| ftp-dl-archive-block | FTP file transfer for DLP archiving was blocked. In DLP archiving, the DLP engine examines email, FTP, IM, NNTP, and web traffic. When enabled, the FortiGate unit records all occurrences of these traffic types when they are detected by the sensor. |
| ftp-dl-blocked | Antivirus <i>File Filter</i> enabled for FTP in an antivirus profile blocks a file being downloaded using FTP that matches an entry in the selected file filter list and sends this message to the FTP client. |
| ftp-dl-dlp-ban | In a DLP sensor, a rule with action set to <i>Ban</i> blocks an FTP session and displays this message. This message is displayed whenever the banned user attempts to access until the user is removed from the banned user list. |

Replacement messages can include replacement message tags. When users receive the replacement message, the replacement message tag is replaced with content relevant to the message.

Table 10: Replacement message tags

| Tag | Description |
|------------------|--|
| %%FILE%% | The name of a file that has been removed from a content stream. This could be a file that contained a virus or was blocked by antivirus file blocking. %%FILE%% can be used in virus and file block messages. |
| %%VIRUS%% | The name of a virus that was found in a file by the antivirus system. %%VIRUS%% can be used in virus messages |
| %%QUARFILENAME%% | The name of a file that has been removed from a content stream and added to the quarantine. This could be a file that contained a virus or was blocked by antivirus file blocking. %%QUARFILENAME%% can be used in virus and file block messages. Quarantining is only available on FortiGate units with a local disk. |
| %%URL%% | The URL of a web page. This can be a web page that is blocked by web filter content or URL blocking. %%URL%% can also be used in http virus and file block messages to be the URL of the web page from which a user attempted to download a file that is blocked. |
| %%PROTOCOL%% | The protocol (HTTP, FTP, POP3, IMAP, SMTP) in which a virus was detected. %%PROTOCOL%% is added to alert email virus messages. |
| %%SOURCE_IP%% | The IP address from which a virus was received. For email this is the IP address of the email server that sent the email containing the virus. For HTTP this is the IP address of the web page that sent the virus. |
| %%DEST_IP%% | The IP address of the computer that would have received the blocked file. For email this is the IP address of the user's computer that attempted to download the message from which the file was removed. |

replacemsg http

Use this command to change default replacement messages added to web pages when the antivirus engine blocks a file in an HTTP session because of a matching file pattern or because a virus is detected; or when web filter blocks a web page.

The FortiGate unit sends the HTTP replacement messages listed to web browsers using the HTTP protocol when an event occurs such as antivirus blocking a file that contains a virus in an HTTP session. HTTP replacement messages are HTML pages.

If the FortiGate unit supports SSL content scanning and inspection these replacement messages can also replace web pages downloaded using the HTTPS protocol.

Syntax

```
config system replacemsg http <message-type>
    set buffer <message>
    set format <format>
    set header <header_type>
end
```

| Variable | Description | Default |
|----------------------|---|--------------------------|
| <message-type> | HTTP replacement message type. See Table 11 . | No default. |
| buffer <message> | Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters. | Depends on message type. |
| format <format> | Set the format of the message: html text none | No default |
| header <header_type> | Set the format of the message header: 8bit http none | Depends on message type. |

Table 11: HTTP replacement messages

| Message name | Description |
|--------------------|--|
| bannedword | Web content blocking is enabled in a web filter profile, and blocks a web page being downloaded with an HTTP GET that contains content matching an entry in the selected Web Content Block list. The blocked page is replaced with the <code>bannedword</code> web page. |
| http-archive-block | A transfer contained a blocked DLP archive. In DLP archiving, the DLP engine examines email, FTP, IM, NNTP, and web traffic. When enabled, the FortiGate unit records all occurrences of these traffic types when they are detected by the sensor. |

Table 11: HTTP replacement messages

| Message name | Description |
|---------------------------|--|
| http-block | Antivirus <i>File Filter</i> is enabled for HTTP or HTTPS in a web filter profile, and blocks a file being downloaded using an HTTP GET that matches an entry in the selected file filter list. The file is replaced with the <code>http-block</code> web page that is displayed by the client browser. |
| http-client-archive-block | The user is not allowed to upload the file. |
| http-client-bannedword | Web content blocking enabled in a web filter profile blocks a web page being uploaded with an HTTP PUT that contains content that matches an entry in the selected Web Content Block list. The client browser displays the <code>http-client-bannedword</code> web page. |
| http-client-block | Antivirus <i>File Filter</i> is enabled for HTTP or HTTPS in an antivirus profile blocks a file being uploaded by an HTTP POST that matches an entry in the selected file filter list and replaces it with the <code>http-client-block</code> web page that is displayed by the client browser. |
| http-client-filesize | <i>Oversized File/Email</i> is set to <i>Block</i> for HTTP or HTTPS and an oversized file that is being uploaded with an HTTP PUT is blocked and replaced with the <code>http-client-filesize</code> web page. |
| http-contenttype-block | When a specific type of content is not allowed, it is replaced with the <code>http-contenttype-block</code> web page. |
| http-dlp-ban | In a DLP sensor, a rule with action set to <i>Ban</i> replaces a blocked web page or file with the <code>http-dlp-ban</code> web page. This web page also replaces any additional web pages or files that the banned user attempts to access until the user is removed from the banned user list. |
| http-filesize | Antivirus <i>Oversized File/Email</i> is set to <i>Block</i> for HTTP or HTTPS and blocks an oversized file being downloaded using an HTTP GET. The file is replaced with the <code>http-filesize</code> web page that is displayed by the client browser. |
| http-post-block | <i>HTTP POST Action</i> is set to <i>Block</i> and the FortiGate unit blocks an HTTP POST and displays the <code>http-post-block</code> web page. |
| https-invalid-cert-block | When an invalid security certificate is detected, the <code>https-invalid-cert-block</code> page is displayed. |
| infcache-block | Client comforting is enabled and the FortiGate unit blocks a URL added to the client comforting URL cache. It replaces the blocked URL with the <code>infcache-block</code> web page. For more information about the client comforting URL cache, see “firewall policy, policy6” on page 167 . |
| url-block | Web URL filtering is enabled and blocks a web page with a URL that matches an entry in the selected URL Filter list. The blocked page is replaced with the <code>url-block</code> web page. |

Replacement messages can include replacement message tags. When users receive the replacement message, the replacement message tag is replaced with content relevant to the message.

Table 12: Replacement message tags

| Tag | Description |
|------------------|--|
| %%FILE%% | The name of a file that has been removed from a content stream. This could be a file that contained a virus or was blocked by antivirus file blocking. %%FILE%% can be used in virus and file block messages. |
| %%VIRUS%% | The name of a virus that was found in a file by the antivirus system. %%VIRUS%% can be used in virus messages |
| %%QUARFILENAME%% | The name of a file that has been removed from a content stream and added to the quarantine. This could be a file that contained a virus or was blocked by antivirus file blocking. %%QUARFILENAME%% can be used in virus and file block messages. Quarantining is only available on FortiGate units with a local disk. |
| %%URL%% | The URL of a web page. This can be a web page that is blocked by web filter content or URL blocking. %%URL%% can also be used in http virus and file block messages to be the URL of the web page from which a user attempted to download a file that is blocked. |
| %%PROTOCOL%% | The protocol (HTTP, FTP, POP3, IMAP, SMTP) in which a virus was detected. %%PROTOCOL%% is added to alert email virus messages. |
| %%SOURCE_IP%% | The IP address of the web page from which a virus was received. |
| %%DEST_IP%% | The IP address of the computer that would have received the blocked file. For email this is the IP address of the user's computer that attempted to download the message from which the file was removed. |

replacemsg im

Use this command to change default replacement messages added to instant messaging and peer-to-peer sessions when either file-transfer or voice-chat is blocked.

By default, these are text messages with an 8-bit header.

Syntax

```
config system replacemsg im <message-type>
  set buffer <message>
  set format <format>
  set header <header_type>
end
```

| Variable | Description | Default |
|----------------------|---|--------------------------|
| <message-type> | im replacement message type. See Table 13 . | No default. |
| buffer <message> | Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters. | Depends on message type. |
| format <format> | Set the format of the message: html text none | No default |
| header <header_type> | Set the format of the message header: 8bit http none | Depends on message type. |

Table 13: Instant messaging (IM) and peer to peer (P2P) message types

| Message name | Description |
|-----------------------|---|
| im-dlp | In a DLP sensor, a rule with action set to <i>Block</i> replaces a blocked IM or P2P message with this message. |
| im-dlp-ban | In a DLP sensor, a rule with action set to <i>Ban</i> replaces a blocked IM or P2P message with this message. This message also replaces any additional messages that the banned user sends until they are removed from the banned user list. |
| im-file-xfer-block | Antivirus <i>File Filter</i> enabled for IM deletes a file that matches an entry in the selected file filter list and replaces it with this message. |
| im-file-xfer-infected | Antivirus <i>Virus Scan</i> enabled for IM deletes an infected file from and replaces the file with this message. |
| im-file-xfer-name | Antivirus <i>File Filter</i> enabled for IM deletes a file with a name that matches an entry in the selected file filter list and replaces it with this message. |

Table 13: Instant messaging (IM) and peer to peer (P2P) message types

| Message name | Description |
|----------------------|--|
| im-file-xfer-size | Antivirus <i>Oversized File/Email</i> set to <i>Block</i> for IM removes an oversized file and replaces the file with this message. |
| im-long-chat-block | In an Application Control list, the <code>block-long-chat</code> CLI field is enabled for AIM, ICQ, MSN, or Yahoo. You enable blocking oversized chat messages from the CLI. |
| im-photo-share-block | In an Application Control list, the <code>block-photo</code> CLI field is enabled for MSN, or Yahoo. You enable photo blocking from the CLI. |
| im-voice-chat-block | In an Application Control list, the <i>Block Audio</i> option is selected for AIM, ICQ, MSN, or Yahoo!. |
| im-video-chat-block | In an Application Control list, the <code>block-video</code> CLI field is enabled for MSN. You enable video chat blocking from the CLI. |

Replacement messages can include replacement message tags. When users receive the replacement message, the replacement message tag is replaced with content relevant to the message.

Table 14: Replacement message tags

| Tag | Description |
|------------------|--|
| %%FILE%% | The name of a file that has been removed from a content stream. This could be a file that contained a virus or was blocked by antivirus file blocking. %%FILE%% can be used in virus and file block messages. |
| %%VIRUS%% | The name of a virus that was found in a file by the antivirus system. %%VIRUS%% can be used in virus messages |
| %%QUARFILENAME%% | The name of a file that has been removed from a content stream and added to the quarantine. This could be a file that contained a virus or was blocked by antivirus file blocking. %%QUARFILENAME%% can be used in virus and file block messages. Quarantining is only available on FortiGate units with a local disk. |
| %%PROTOCOL%% | The protocol (HTTP, FTP, POP3, IMAP, SMTP) in which a virus was detected. %%PROTOCOL%% is added to alert email virus messages. |
| %%SOURCE_IP%% | The IP address from which a virus was received. For email this is the IP address of the email server that sent the email containing the virus. For HTTP this is the IP address of the web page that sent the virus. |
| %%DEST_IP%% | The IP address of the computer that would have received the blocked file. For email this is the IP address of the user's computer that attempted to download the message from which the file was removed. |

replacemsg mail

Use this command to change default replacement messages added to email messages when the antivirus engine blocks a file either because of a matching file pattern or because a virus is detected; or when spam filter blocks an email.

By default, these are text messages with an 8-bit header.

Syntax

```
config system replacemsg mail <message-type>
    set buffer <message>
    set format <format>
    set header <header_type>
end
```

| Variable | Description | Default |
|----------------------|---|--------------------------|
| <message-type> | mail replacement message type. See Table 15 . | No default. |
| buffer <message> | Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters. | Depends on message type. |
| format <format> | Set the format of the message: html text none | No default |
| header <header_type> | Set the format of the message header: 8bit http none | Depends on message type. |

Table 15: mail message types

| Message name | Description |
|---------------------|---|
| email-block | The antivirus <i>File Filter</i> is enabled for an email protocol deletes a file that matches an entry in the selected file filter list. The file is blocked and the email is replaced with the <code>email-block</code> message. |
| email-dlp-ban | In a DLP sensor, a rule with action set to <i>Ban</i> replaces a blocked email message with this message. This message also replaces any additional email messages that the banned user sends until they are removed from the banned user list. |
| email-dl-ban-sender | In a DLP sensor, a rule with action set to <i>Ban Sender</i> replaces a blocked email message with this message. The <code>email-dlp-ban</code> message also replaces any additional email messages that the banned user sends until the user is removed from the banned user list. |

Table 15: mail message types

| Message name | Description |
|-------------------|---|
| email-dlp-subject | The email-dlp-subject message is added to the subject field of all email messages replaced by the DLP sensor <i>Block</i> , <i>Ban</i> , <i>Ban Sender</i> , <i>Quarantine IP address</i> , and <i>Quarantine interface</i> actions. |
| email-filesize | When the antivirus <i>Oversized File/Email</i> is set to <i>Block</i> for an email protocol removes an oversized file from an email message, the file is replaced with the email-filesize message. |
| partial | Antivirus <i>Pass Fragmented Emails</i> is not enabled so a fragmented email is blocked. The partial message replaces the first fragment of the fragmented email. |
| smtp-block | Splice mode is enabled and the antivirus file filter deleted a file from an SMTP email message. The FortiGate unit aborts the SMTP session and returns a 554 SMTP error message to the sender that includes the smtp-block replacement message. |
| smtp-filesize | Splice mode is enabled and antivirus <i>Oversized File/Email</i> is set to <i>Block</i> . When the FortiGate unit blocks an oversize SMTP email message, the FortiGate unit aborts the SMTP session and returns a 554 SMTP error message to the sender that includes the smtp-filesize replacement message. |

Replacement messages can include replacement message tags. When users receive the replacement message, the replacement message tag is replaced with content relevant to the message.

Table 16: Replacement message tags

| Tag | Description |
|------------------|--|
| %%FILE%% | The name of a file that has been removed from a content stream. This could be a file that contained a virus or was blocked by antivirus file blocking. %%FILE%% can be used in virus and file block messages. |
| %%VIRUS%% | The name of a virus that was found in a file by the antivirus system. %%VIRUS%% can be used in virus messages |
| %%QUARFILENAME%% | The name of a file that has been removed from a content stream and added to the quarantine. This could be a file that contained a virus or was blocked by antivirus file blocking. %%QUARFILENAME%% can be used in virus and file block messages. Quarantining is only available on FortiGate units with a local disk. |
| %%PROTOCOL%% | The protocol (HTTP, FTP, POP3, IMAP, SMTP) in which a virus was detected. %%PROTOCOL%% is added to alert email virus messages. |
| %%SOURCE_IP%% | IP address of the email server that sent the email containing the virus. |
| %%DEST_IP%% | IP address of the user's computer that attempted to download the message from which the file was removed. |

Table 16: Replacement message tags

| Tag | Description |
|----------------|--|
| %%EMAIL_FROM%% | The email address of the sender of the message from which the file was removed. |
| %%EMAIL_TO%% | The email address of the intended receiver of the message from which the file was removed. |

replacemsg mm1

Use this command to change default replacement messages added to messages sent by FortiOS Carrier on the MM1 network when the antivirus engine blocks a file either because of a matching file pattern or because a virus is detected; or when spam filter blocks an email.

Syntax

```
config system replacemsg mm1 <message_type>
  set add-smil {enable | disable}
  set charset <character_set>
  set class <class>
  set format <format>
  set from <from_address>
  set from-sender {enable | disable}
  set header <header_type>
  set image <string>
  set message <message_text>
  set priority <priority>
  set rsp-status <rsp_status>
  set rsp-text <response_text>
  set sender-visibility <sender_vis>
  set smil-part <string>
  set subject <subject_text>
end
```

| Variable | Description | Default |
|----------------|--|-------------|
| <message_type> | MM1 replacement message types, one of: mm1-retr-conf-block mm1-retr-conf-bword mm1-retr-conf-sis-block mm1-retr-conf-virus mm1-send-conf-block mm1-send-conf-bword mm1-send-conf-sis-block mm1-send-conf-virus mm1-send-req-block mm1-send-req-bword mm1-send-req-sis-block mm1-send-req-virus | No default. |

| | | |
|-----------------------------------|---|--------------------------|
| add-smil {enable disable} | Enable to add SMIL content to the message. SMIL content can include images. This field is available for the following message types: mm1-send-req-block mm1-send-req-bword mm1-send-req-sis-block mm1-send-req-virus | disable |
| charset <character_set> | Character encoding used for replacement message, one of: us-ascii utf-8 | utf-8 |
| class <class> | The message can be classified as one of: advertisement automatic informational not-included personal | automatic |
| format <format> | Set the format of the message, one of: html none text wml Not all formats are supported by all message types. | text |
| from <from_address> | Address the message is from. | null |
| from-sender {enable disable} | Enable for the notification message to be sent from the recipient. This is to avoid billing problems. | disable |
| header <header_type> | Set the format of the message header, one of: 8bit http none | http |
| image <string> | Enter the name of the image to include in the SMIL message part. Using '?' will show the list of available image names. This is only available when add-smil is enabled. | |
| message <message_text> | Text of the replacement message. | Depends on message type. |

| | | |
|-----------------------------------|---|--------------------------|
| priority <priority> | Priority of the message, one of: high low normal not included | normal |
| rsp-status <rsp_status> | Response status code, one of: err-content-not-accepted err-msg-fmt-corrupt err-msg-not-found err-net-prob err-snd-addr-unresolv err-srv-denied err-unspecified err-unsupp-msg ok | err-content-not-accepted |
| rsp-text <response_text> | Response text. | Depends on message type. |
| sender-visibility <sender_vis> | Sender visibility, one of: hide not-specified show | not-specified |
| smil-part <string> | Enter the SMIL part of the replacement message. | |
| subject <subject_text> | Subject text string. | Depends on message type. |

replacemsg mm3

Use this command to change default replacement messages added to messages sent by FortiOS Carrier on the MM3 network when the antivirus engine blocks a file either because of a matching file pattern or because a virus is detected; or when spam filter blocks an email.

Syntax

```
config system replacemsg mm3 <message_type>
  set charset <character_set>
  set format <format>
  set from <from_address>
  set header <header_type>
  set message <message_text>
  set priority <priority>
  set subject <subject_text>
end
```

| Variable | Description | Default |
|-------------------------|---|-------------|
| <message_type> | MM3 replacement message types, one of: mm3-block mm3-block-notif mm3-bword mm3-bword-notif mm3-sis-block mm3-sis-block-notif mm3-sis-block-notif mm3-virus mm3-virus-block | No default. |
| charset <character_set> | Character encoding used for replacement messages, one of: us-ascii utf-8 | utf-8 |
| format <format> | Replacement message format flag, one of: html none text wml | text |
| from <from_address> | Address the message is from. | null |
| header <header_type> | Set the format of the message header, one of: 8bit http none | none |

| | | |
|---------------------------|---|-----------------------------|
| message <message_text> | Text of the replacement message. | Depends on message type. |
| priority <priority> | Priority of the message, one of: high low normal not included | normal |
| subject <subject_text> | Subject text string. | Depends on message type. |

replacemsg mm4

Use this command to change default replacement messages added to messages sent by FortiOS Carrier on the MM4 network when the antivirus engine blocks a file either because of a matching file pattern or because a virus is detected; or when spam filter blocks an email.

Syntax

```
config system replacemsg mm4 <message_type>
  set charset <character_set>
  set class <class>
  set domain <address_domain>
  set format <format>
  set from <from_address>
  set from-sender {enable | disable}
  set header <header_type>
  set image <string>
  set message <message_text>
  set priority <priority>
  set rsp-status <rsp_status>
  set smil-part <string>
  set subject <subject_text>
end
```

| Variable | Description | Default |
|--------------------------------|--|-------------|
| <message_type> | MM4 replacement message types, one of: mm4-block mm4-block-notif mm4-bword mm4-bword-notif mm4-sis-block mm4-sis-block-notif mm4-virus mm4-virus-block | No default. |
| add-smil {enable disable} | Enable to add SMIL content to the message. SMIL content can include images. This field is available for the following message types: mm4-block-notif mm4-bword-notif mm4-sis-block-notif | disable |
| charset <character_set> | Character encoding used for replacement messages: us-ascii or utf-8. | utf-8 |

| | | |
|-----------------------------------|---|--------------------------|
| class <class> | The message can be classified as one of: advertisement automatic informational not-included personal | automatic |
| domain <address_domain> | The from address domain. | null |
| format <format> | Replacement message format flag, one of: html none text wml | text |
| from <from_address> | Address the message is from. | null |
| from-sender {enable disable} | Enable for the notification message to be sent from the recipient. This is to avoid billing problems. | disable |
| header <header_type> | Set the format of the message header: 8bit, http, or none. | none |
| image <string> | Enter the name of the image to include in the SMIL message part. Using '?' will show the list of available image names. This is only available when add-smil is enabled. | |
| message <message_text> | Text of the replacement message. | Depends on message type. |
| priority <priority> | Priority of the message, one of: high low normal not included | normal |
| rsp-status <rsp_status> | Response status codes, one of: err-content-not-accepted err-msg-fmt-corrupt err-net-prob err-snd-addr-unresolv err-srv-denied err-unspecified err-unsupp-msg ok | err-content-not-accepted |
| smil-part <string> | Enter the SMIL part of the replacement message. | |
| subject <subject_text> | Subject text string. | Depends on message type. |

replacemsg mm7

Use this command to change default replacement messages added to messages sent by FortiOS Carrier on the MM7 network when the antivirus engine blocks a file either because of a matching file pattern or because a virus is detected; or when spam filter blocks an email.

Syntax

```
config system replacemsg mm7 <mm7message_type>
    set add-smil {enable | disable}
    set addr_type <addr_type>
    set charset <character_set>
    set class <class>
    set format <format>
    set from <from_address>
    set from-sender {enable | disable}
    set header <header_type>
    set image <string>
    set message <message_text>
    set priority <priority>
    set rsp-status <rsp_status>
    set smil-part <string>
    set subject <subject_text>
end
```

| Variable | Description | Default |
|--------------------------------|--|-------------|
| <mm7message_type> | MM7 replacement message types, one of: mm7-block mm7-block-notif mm7-bword mm7-bword-notif mm7-sis-block mm7-sis-block-notif mm7-virus mm7-virus-block | No default. |
| add-smil {enable disable} | Enable to add SMIL content to the message. SMIL content can include images. This field is available for the following message types: mm7-block-notif mm7-bword-notif mm7-sis-block-notif | disable |
| addr_type <addr_type> | From address types, one of: number rfc2882-addr short-code | number |

| | | |
|-------------------------------------|---|-----------------------------|
| charset <character_set> | Character encoding used for replacement messages, one of: us-ascii utf-8 | utf-8 |
| class <class> | The message can be classified as one of: advertisement automatic informational not-included personal | automatic |
| format <format> | Replacement message format flag, one of: html none text wml | text |
| from <from_address> | Address the message is from. | null |
| from-sender { enable disable } | Enable for the notification message to be sent from the recipient. This is to avoid billing problems. | disable |
| header <header_type> | Set the format of the message header, one of: 8bit http none | none |
| image <string> | Enter the name of the image to include in the SMIL message part. Using '?' will show the list of available image names. This is only available when add-smil is enabled. | |
| message <message_text> | Text of the replacement message. | Depends on message type. |
| priority <priority> | Priority of the message, one of: high low normal not included | normal |

| | | |
|----------------------------|---|--------------------------|
| rsp-status <rsp_status> | Response status codes, one of: addr-err addr-not-found app-addr-not-supp app-denied app-id-not-found client-err content-refused gen-service-err improper-ident link-id-not-found msg-fmt-corrupt msg-id-not-found msg-rejected multiple-addr-not-supp not-possible oper-restrict partial-success repl-app-id-not-found service-denied service-err service-unavail srv-err success unsupp-oper unsupp-ver validation-err | Depends on message type. |
| smil-part <string> | Enter the SMIL part of the replacement message. | |
| subject <subject_text> | Subject text string. | Depends on message type. |

replacemsg-group

Use this command to define replacement messages for your VDOM, overriding the corresponding global replacement messages.

Syntax

To create a VDOM-specific replacement message:

```
config system replacemsg-group
edit default
config <msg_category>
edit <msg_type>
set buffer <message>
set format <format>
set header <header_type>
end
end
```

To remove a VDOM-specific replacement message, restoring the global replacement message:

```
config system replacemsg-group
edit default
config <msg_category>
delete <msg_type>
end
```

| Variable | Description | Default |
|-----------------------|---|--------------------------|
| buffer <message> | Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters. | Depends on message type. |
| comment <comment_str> | Optionally, enter a descriptive comment. | No default |
| format <format> | Set the format of the message: html text none | No default |
| header <header_type> | Set the format of the message header: 8bit http none | Depends on message type. |

| Variable | Description | Default |
|----------------|---|------------|
| <msg_category> | The category of replacement message. This corresponds to the field following <code>replacemsg</code> in the global <code>system replacemsg</code> command. For example, the <code>http</code> category includes the messages defined globally in the <code>system replacemsg http</code> command. | No default |
| <msg_type> | The message type. This corresponds to the final field in the global <code>system replacemsg</code> command. For example, to create a new login message for your SSL VPN, you would set <msg_category> to <code>sslvpn</code> and <msg_type> to <code>sslvpn-login</code> . | No default |

replacemsg-group

Replacement messages can be created and applied to specific profile groups. This allows the customization of messages for specific users or user groups.

If a user is not part of a custom replacement message group, their replacement messages come from the 'default' group. The 'default' group always exists, and cannot be deleted. All additional replacement message groups inherit from the default group. Any messages in custom groups that have not been modified, inherit any changes to those messages in the default group.

The only replacement messages that can not be customized in groups are administration related messages, which in the following categories:

- Alert Mail
- Administration
- Authentication
- IM and P2P
- SSL VPN

Except for mm1, mm3, mm4, mm7 which use the `message` field, all replacement message types use the `buffer` field to refer to the body of the message.

Syntax

```
config system replacemsg-group
  edit <groupname_string>
    set comment <string>
    set group-type {auth | captive-portal | ec | utm}
    config {auth | ec | fortiguard-wf | ftp | http | mail | mm1
      | mm3 | mm4 | mm7 | nntp | spam}
    edit <msgkey_integer>
      set msg-type <type>
      set buffer <string>
      set header <header_flag>
      set format <format_flag>
      set message <string>
    end
  end
end
```

| Variable | Description | Default |
|-------------------------|---|---------|
| edit <groupname_string> | Create or edit a replacement message group. Use a groupname of <code>default</code> to configure per-vdom replacement messages. Only valid when VDOMs are enabled. | |
| comment <string> | Enter a descriptive comment for this replacement message group. | |

| Variable | Description | Default |
|---|---|---------|
| group-type { auth captive-portal ec utm } | <p>Enter the type of replacement message group this is.</p> <p>auth — for use with authentication pages in firewall policies</p> <p>captive-portal — for use with captive-portal configurations</p> <p>ec — for use with endpoint-control profiles</p> <p>utm — for use with UTM settings in firewall policies</p> <p>default — used to configure per-vdom replacement messages, only available when group name is set to default</p> | utm |
| config { auth ec fortiguard-wf ftp http mail mm1 mm3 mm4 mm7 nntp spam } | <p>Select a replacement message type to add or edit. These types or protocols, match with the existing replacemsg commands, and determine which msg-types are available.</p> <p>For more information on these replacement message types see:</p> <ul style="list-style-type: none"> • “system replacemsg auth” on page 613 • “system replacemsg ec” on page 618 • “replacemsg fortiguard-wf” on page 620 • “replacemsg ftp” on page 622 • “replacemsg http” on page 624 • “replacemsg mail” on page 629 • “replacemsg mm1” on page 632 • “replacemsg mm3” on page 635 • “replacemsg mm4” on page 637 • “replacemsg mm7” on page 639 • “replacemsg nntp” on page 650 • “replacemsg spam” on page 652 <p>Note: mm1,mm3,mm4,and mm7 are FortiOS Carrier only.</p> | |
| edit <msgkey_integer> | <p>Create or edit a message entry in the table. Enter the key of the entry.</p> <p>Using ‘?’ will show you the existing message type as well as the msgkey entries in the table.</p> | |
| msg-type <type> | <p>Select the message type for this message entry. Valid message types vary according to which replacement message table you are editing.</p> <p>For a list of valid message types for this table, refer to the CLI replacemsg command of the same name.</p> | |

| Variable | Description | Default |
|----------------------|---|---------|
| buffer <string> | Enter the replacement message for this message type. Enclose the message in quotes. This field is used with the following replacement messages: fortiguard-wf ftp http mail nntp spam Other replacement messages use the <code>message</code> field. | |
| header <header_flag> | Select the header for this message. Valid types include: 8bit http none | |
| format <format_flag> | Select the format of this message. Valid formats include: html none text wml (FortiOS Carrier only) | |
| message <string> | Enter the replacement message for this message type. Enclose the message in quotes. This field is used with the following replacement messages: mm1 (FortiOS Carrier only) mm3 (FortiOS Carrier only) mm4 (FortiOS Carrier only) mm7 (FortiOS Carrier only) Other replacement messages use the <code>buffer</code> field. | |

replacemsg-image

Use this command to add, edit, or delete images to be used in HTTP replacement messages and for the SMIL parts of FortiOS Carrier replacement messages. Both image-base64 and image-type must be present for a valid entry.

Syntax

```
config system replacemsg-image
  edit <image_name>
    set image-base64 <image_data>
    set image-type <format>
  end
```

| Variable | Description | Default |
|---------------------------|---|---------|
| edit <image_name> | Enter the name or tag to use for this image | none. |
| image-base64 <image_data> | Enter the image in base64 encoding. You can also use the graphical interface to add images by browsing to their location. | none. |
| image-type <format> | Select the format of the image. Available formats include: gif jpeg png tiff | none. |

replacemsg nac-quar

Use this command to change the NAC quarantine pages for data leak (DLP), denial of service (DoS), IPS, and virus detected.

These are HTML messages with HTTP headers.

Syntax

```
config system replacemsg nac-quar nac-quar_msg_type
    set buffer <message>
    set format <format>
    set header <header_type>
end
```

| Variable | Description | Default |
|----------------------|---|--------------------------|
| nac-quar_msg_type | Replacement message type. See Table 17 . | No default |
| buffer <message> | Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters. | Depends on message type. |
| format <format> | Set the format of the message: html text none | No default |
| header <header_type> | Set the format of the message header: 8bit http none | Depends on message type. |

Table 17: nac-quar message types

| Message name | Description |
|--------------|---|
| nac-quar-dlp | Action set to <i>Quarantine IP address</i> or <i>Quarantine Interface</i> in a DLP sensor and the DLP sensor adds a source IP address or a FortiGate interface to the banned user list. The FortiGate unit displays this replacement message as a web page when the blocked user attempts to connect through the FortiGate unit using HTTP on port 80 or when any user attempts to connect through a FortiGate interface added to the banned user list using HTTP on port 80. |
| nac-quar-dos | For a DoS Sensor the CLI <i>quarantine</i> option set to <i>attacker</i> or <i>interface</i> and the DoS Sensor added to a DoS firewall policy adds a source IP, a destination IP, or FortiGate interface to the banned user list. The FortiGate unit displays this replacement message as a web page when the blocked user attempts to connect through the FortiGate unit using HTTP on port 80 or when any user attempts to connect through a FortiGate interface added to the banned user list using HTTP on port 80. This replacement message is not displayed if <i>quarantine</i> is set to <i>both</i> . |

Table 17: nac-quar message types

| Message name | Description |
|----------------|---|
| nac-quar-ips | <i>Quarantine Attackers</i> enabled in an IPS sensor filter or override and the IPS sensor adds a source IP address, a destination IP address, or a FortiGate interface to the banned user list. The FortiGate unit displays this replacement message as a web page when the blocked user attempts to connect through the FortiGate unit using HTTP on port 80 or when any user attempts to connect through a FortiGate interface added to the banned user list using HTTP on port 80. This replacement message is not displayed if <i>method</i> is set to <i>Attacker and Victim IP Address</i> . |
| nac-quar-virus | <i>Antivirus Quarantine Virus Sender</i> adds a source IP address or FortiGate interface to the banned user list. The FortiGate unit displays this replacement message as a web page when the blocked user attempts to connect through the FortiGate unit using HTTP on port 80 or when any user attempts to connect through a FortiGate interface added to the banned user list using HTTP on port 80. |

replacemsg nntp

Use this command to change the net news transfer protocol (NNTP) download pages.

These are HTML messages with HTTP headers.

Syntax

```
config system replacemsg nntp auth_msg_type
    set buffer <message>
    set format <format>
    set header <header_type>
end
```

| Variable | Description | Default |
|----------------------|---|--------------------------|
| auth_msg_type | FortiGuard replacement alertmail message type. See Table 18 . | No default |
| buffer <message> | Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters. | Depends on message type. |
| format <format> | Set the format of the message: html text none | No default |
| header <header_type> | Set the format of the message header: 8bit http none | Depends on message type. |

Table 18: net news transfer protocol (NNTP) message types

| Message name | Description |
|------------------|---|
| nntp-dl-blocked | Antivirus <i>File Filter</i> is enabled for NNTP blocks a file attached to an NNTP message that matches an entry in the selected file filter list. The FortiGate unit sends the nntp-dl-blocked message to the FTP client. |
| nntp-dl-filesize | Antivirus <i>Oversized File/Email</i> is set to <i>Block</i> for NNTP. The FortiGate unit removes an oversized file from an NNTP message and replaces the file with the nntp-dl-filesize message. |
| nntp-dlp-ban | In a DLP sensor, a rule with action set to <i>Ban</i> replaces a blocked NNTP message with this message. The nntp-dlp-ban message also replaces any additional NNTP messages that the banned user sends until they are removed from the banned user list. |
| nntp-dlp-subject | The nntp-dlp-subject message is added to the subject field of all NNTP messages replaced by the DLP sensor <i>Block</i> , <i>Ban</i> , <i>Quarantine IP address</i> , and <i>Quarantine interface</i> actions. |

Replacement messages can include replacement message tags. When users receive the replacement message, the replacement message tag is replaced with content relevant to the message.

Table 19: Replacement message tags

| Tag | Description |
|------------------|--|
| %%FILE%% | The name of a file that has been removed from a content stream. This could be a file that contained a virus or was blocked by antivirus file blocking. The file may have been quarantined if a virus was detected. %%FILE%% can be used in virus and file block messages. |
| %%QUARFILENAME%% | The name of a file that has been removed from a content stream and added to the quarantine. This could be a file that contained a virus or was blocked by antivirus file blocking. %%QUARFILENAME%% can be used in virus and file block messages. Quarantining is only available on FortiGate units with a local disk. |
| %%VIRUS%% | The name of a virus that was found in a file by the antivirus system. %%VIRUS%% can be used in virus messages |

replacemsg spam

The FortiGate unit adds the Spam replacement messages listed in [Table 20](#) to SMTP server responses if the email message is identified as spam and the spam action is discard. If the FortiGate unit supports SSL content scanning and inspection these replacement messages can also be added to SMTPS server responses.

By default, these are text messages with an 8-bit header.

Syntax

```
config system replacemsg spam <message-type>
    set buffer <message>
    set format <format>
    set header <header_type>
end
```

| Variable | Description | Default |
|----------------------|---|--------------------------|
| <message-type> | Spam replacement message type. See Table 20 . | No default. |
| buffer <message> | Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters. | Depends on message type. |
| format <format> | Set the format of the message, one of: html text none | text |
| header <header_type> | Set the format of the message header, one of: 8bit http none | 8bit |

Table 20: spam message types

| Message name | Description |
|----------------------|--|
| ipblocklist | Spam Filtering <i>IP address BWL check</i> enabled for an email protocol identifies an email message as spam and adds this replacement message. |
| reversedns | Spam Filtering <i>Return e-mail DNS check</i> enabled for an email protocol identifies an email message as spam and adds this replacement message. |
| smtp-spam-ase | The FortiGuard Antispam Engine (ASE) reports this message as spam. |
| smtp-spam-bannedword | Spam Filtering <i>Banned word check</i> enabled for an email protocol identifies an email message as spam and adds this replacement message. |

Table 20: spam message types

| Message name | Description |
|----------------------|--|
| smtp-spam-dnsbl | From the CLI, <code>spamrbl</code> enabled for an email protocol identifies an email message as spam and adds this replacement message. |
| smtp-spam-emailblack | The spam filter email address blacklist marked an email as spam. The <code>smtp-spam-emailblack</code> replaces the email. |
| smtp-spam-feip | FortiGuard Antispam IP address checking identifies an email message as spam and adds this replacement message to the server response. |
| smtp-spam-helo | Spam Filtering <i>HELO DNS lookup</i> enabled for SMTP identifies an email message as spam and adds this replacement message. <i>HELO DNS lookup</i> is not available for SMTPS. |
| smtp-spam-mimeheader | From the CLI, <code>spamdrccheck</code> enabled for an email protocol identifies an email message as spam and adds this replacement message. |
| submit | Any Spam Filtering option enabled for an email protocol identifies an email message as spam and adds this replacement message. Spam Filtering adds this message to all email tagged as spam. The message describes a button that the recipient of the message can select to submit the email signatures to the FortiGuard Antispam service if the email was incorrectly tagged as spam (a false positive). |

Table 21: Replacement messages can include replacement message tags. When users receive the replacement message, the replacement message tag is replaced with content relevant to the message.**Table 22:** Replacement message tags

| Tag | Description |
|------------------|---|
| %%QUARFILENAME%% | The name of a file that has been removed from a content stream and added to the quarantine. This could be a file that contained a virus or was blocked by antivirus file blocking. %%QUARFILENAME%% can be used in virus and file block messages. Quarantining is only available on FortiGate units with a local disk. |
| %%SOURCE_IP%% | The IP address from which a virus was received. For email this is the IP address of the email server that sent the email containing the virus. For HTTP this is the IP address of the web page that sent the virus. |
| %%DEST_IP%% | The IP address of the computer that would have received the blocked file. For email this is the IP address of the user's computer that attempted to download the message from which the file was removed. |

Table 22: Replacement message tags

| Tag | Description |
|----------------|--|
| %%EMAIL_FROM%% | The email address of the sender of the message from which the file was removed. |
| %%EMAIL_TO%% | The email address of the intended receiver of the message from which the file was removed. |

replacemsg sslvpn

The SSL VPN login replacement messages are HTML replacement messages.

The `sslvpn-login` message formats the FortiGate SSL VPN portal login page.

The `sslvpn-limit` message formats the web page that appears if a user attempts to log into SSL VPN more than once.

You can customize these replacement messages according to your organization’s needs. The pages are linked to FortiGate functionality and you must construct them according to the following guidelines to ensure that it will work.

These are HTML messages with HTTP headers.

Syntax

```
config system replacemsg sslvpn {sslvpn-limit | sslvpn-login}
    set buffer <message>
    set format <format>
    set header <header_type>
end
```

| Variable | Description | Default |
|----------------------|---|--------------------------|
| buffer <message> | Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters. | Depends on message type. |
| format <format> | Set the format of the message: html text none | No default |
| header <header_type> | Set the format of the message header: 8bit http none | Depends on message type. |

Replacement messages can include replacement message tags. When users receive the replacement message, the replacement message tag is replaced with content relevant to the message.

replacemsg traffic-quota

When user traffic through the FortiGate unit is blocked by traffic shaper quota controls, users see the *Traffic shaper block message* or the *Per IP traffic shaper block message* when they attempt to connect through the FortiGate unit using HTTP.

This is an HTML message with an HTTP header.

Syntax

```
config system replacemsg traffic-quota {per-ip-shaper-block |  
    traffic-shaper-block}  
    set buffer <message>  
    set format <format>  
    set header <header_type>  
end
```

| Variable | Description | Default |
|----------------------|---|--------------------------|
| buffer <message> | Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters. | Depends on message type. |
| format <format> | Set the format of the message: html text none | No default |
| header <header_type> | Set the format of the message header: 8bit http none | Depends on message type. |

Replacement messages can include replacement message tags. When users receive the replacement message, the replacement message tag is replaced with content relevant to the message.

Requirements for traffic quota pages

The traffic quota HTTP pages should contain the %%QUOTA_INFO%% tag to display information about the traffic shaping quota setting that is blocking the user.

replacemsg utm

When data leaks or viruses are detected, these messages are substituted for the blocked item.

Syntax

```
config system replacemsg utm <message_type>
    set buffer <message>
    set format <format>
    set header <header_type>
end
```

| Variable | Description | Default |
|----------------------|---|--------------------------|
| buffer <message> | Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters. | Depends on message type. |
| format <format> | Set the format of the message: html text none | No default |
| header <header_type> | Set the format of the message header: 8bit http none | Depends on message type. |

| Message Type | Description |
|--------------|--|
| dlp-text | An email message is blocked because it appears to contain a data leak. |
| dlp-html | An HTTP transfer is blocked because it appears to contain a data leak. |
| virus-html | A virus was detected in a file being downloaded using an HTTP GET. |
| virus-text | A virus was detected in a file attachment. The file was removed. |

Table 23: Replacement message tags

| Tag | Description |
|-----------|---|
| %%FILE%% | The name of a file that has been removed from a content stream. This could be a file that contained a virus or was blocked by antivirus file blocking. %%FILE%% can be used in virus and file block messages. |
| %%VIRUS%% | The name of a virus that was found in a file by the antivirus system. %%VIRUS%% can be used in virus messages |

Table 23: Replacement message tags

| Tag | Description |
|------------------|---|
| %%QUARFILENAME%% | The name of a file that has been removed from a content stream and added to the quarantine. This could be a file that contained a virus or was blocked by antivirus file blocking. %%QUARFILENAME%% can be used in virus and file block messages. Quarantining is only available on FortiGate units with a local disk. |
| %%PROTOCOL%% | The protocol (HTTP, FTP, POP3, IMAP, SMTP) in which a virus was detected. %%PROTOCOL%% is added to alert email virus messages. |

replacemsg webproxy

The web proxy returns messages for user authentication failures and HTTP errors.

Syntax

```
config system replacemsg webproxy {auth-authorization | auth-  
    challenge | auth-login | deny | http-err | user-limit}  
set buffer <message>  
set format <format>  
set header <header_type>
```

| Variable | Description | Default |
|----------------------|---|--------------------------|
| buffer <message> | Type a new replacement message to replace the current replacement message. Maximum length 8 192 characters. | Depends on message type. |
| format <format> | Set the format of the message: html text none | html |
| header <header_type> | Set the format of the message header: 8bit http none | http |

The http-err replacement message requires the following tags:

Table 24: Web proxy http-err replacement message tags

| Tag | Description |
|-------------------|--|
| %%HTTP_ERR_CODE%% | The returned HTTP error code, “404” for example. |
| %%HTTP_ERR_DESC%% | The returned HTTP error message, “Not Found” for example. |
| %%PROTOCOL%% | The protocol that applies to the traffic, “http://” for example. |
| %%URL%% | The URL (not including protocol) that caused the error. |

resource-limits

Use this command to configure resource limits that will apply to all VDOMs. When you set a global resource limit, you cannot exceed that resource limit in any VDOM. For example, enter the following command to limit all VDOMs to 100 VPN IPsec Phase 1 Tunnels:

```
config global
  config system resource-limits
    set ipsec-phase1 100
  end
end
```

With this global limit set you can only add a maximum of 100 VPN IPsec Phase 1 Tunnels to any VDOM.

You can also edit the resource limits for individual VDOMs to further limit the number of resources that you can add to individual VDOMs. See [“system vdom-property” on page 698](#).

A resource limit of 0 means no limit. No limit means the resource is not being limited by the resource limit configuration. Instead the resource is being limited by other factors. The FortiGate unit limits dynamic resources by the capacity of the FortiGate unit and can vary depending on how busy the system is. Limits for static resources are set by limitations in the FortiGate configuration as documented in the [FortiGate Maximum Values Matrix](#) document.

The default maximum value for each resource depends on the FortiGate model. Dynamic resources (Sessions, Dial-up Tunnels, and SSL VPN) do not have default maximums so the default maximum for dynamic resources is always 0 (meaning unlimited). Static resources may have a limit set or many be set to 0 meaning they are limited by the resource limit configuration.



If you set the maximum resource usage for a VDOM you cannot reduce the default maximum global limit for all VDOMs below this maximum.

This command is available only when VDOMs are enabled.

Syntax

```
config global
  config system resource-limits
    set custom-service <max_int>
    set dialup-tunnel <max_int>
    set firewall-address <max_int>
    set firewall-addrgrp <max_int>
    set firewall-policy <max_int>
    set ipsec-phase1 <max_int>
    set ipsec-phase2 <max_int>
    set log-disk-quota <max_int>
    set onetime-schedule <max_int>
    set proxy <max_int>
    set recurring-schedule <max_int>
    set service-group <max_int>
    set session <max_int>
    set sslvpn <max_int>
```

```

set user <max_int>
set user-group <max_int>
end
end

```

| Variable | Description | Default |
|---------------------------------|---|---------|
| custom-service <max_int> | Enter the maximum number of firewall custom services. | |
| dialup-tunnel <max_int> | Enter the maximum number of dialup-tunnels. | |
| firewall-address <max_int> | Enter the maximum number of firewall addresses. | |
| firewall-addrgrp <max_int> | Enter the maximum number of firewall address groups. | |
| firewall-policy <max_int> | Enter the maximum number of firewall policies. | |
| ipsec-phase1 <max_int> | Enter the maximum number of IPSec phase1 tunnels. | |
| ipsec-phase2 <max_int> | Enter the maximum number of IPSec phase2 tunnels. | |
| log-disk-quota <max_int> | Enter the maximum amount of log disk space available in MBytes for global log messages. The range depends on the amount of hard disk space available. | |
| onetime-schedule <max_int> | Enter the maximum number of onetime schedules. | |
| proxy <max_int> | <p>Enter the maximum number of users that can be using the explicit proxy at one time.</p> <p>How the number of concurrent explicit proxy users is determined depends on their authentication method:</p> <ul style="list-style-type: none"> For session-based authenticated users, each authenticated user is counted as a single user. Since multiple users can have the same user name, the proxy attempts to identify users according to their authentication membership (based upon whether they were authenticated using RADIUS, LDAP, FSSO, local database etc.). If a user of one session has the same name and membership as a user of another session, the explicit proxy assumes this is one user. For IP Based authentication, or no authentication, or if no explicit proxy security policy has been added, the source IP address is used to determine a user. All sessions from a single source address are assumed to be from the same user. | |
| recurring-schedule <max_int> | Enter the maximum number of recurring schedules. | |
| service-group <max_int> | Enter the maximum number of firewall service groups. | |
| session <max_int> | Enter the maximum number of sessions. | |
| sslvpn <max_int> | Enter the maximum number of sessions. | |
| user <max_int> | Enter the maximum number of users. | |
| user-group <max_int> | Enter the maximum number of user groups. | |

server-probe

Use this command to configure server probing.

Syntax

```
config system server-probe
edit <id>
    set interval <seconds_int>
    set port <port_int>
    set protocol {ping | http-get}
    set response-value <str>
    set retry <tries-Int>
    set server <server_addr>
    set srcintf <interface_name>
    set status {enable | disable}
    set url <url_str>
end
```

| Variable | Description | Default |
|----------------------------|--|-------------|
| interval <seconds_int> | Enter the period in seconds between probe attempts. | 60 |
| port <port_int> | Enter the TCP port for HTTP-Get protocol probe. | 80 |
| protocol {ping http-get} | Select the protocol to use when probing. | ping |
| response-value <str> | Enter the expected server response. This is available when protocol is http-get. | No default. |
| retry <tries-Int> | Enter the number of times to retry unsuccessful probe. | 5 |
| server <server_addr> | Enter the server IP address or FQDN to probe. | No default. |
| srcintf <interface_name> | Enter the interface to which the server is connected. | No default. |
| status {enable disable} | Enable or disable probe. | enable |
| url <url_str> | Enter the URL for HTTP-Get protocol probe. | No default. |

session-helper

FortiGate units use session helpers to process sessions that have special requirements. Session helpers function like proxies by getting information from the session and performing support functions required by the session. For example:

- The SIP session helper looks inside SIP messages and performs NAT (if required) on the IP addresses in the SIP message and opens pinholes to allow media traffic associated with the SIP session to pass through the FortiGate unit.
- The FTP session helper can keep track of multiple connections initiated from a single FTP session. The session helper can also permits an FTP server to actively open a connection back to a client program.
- The TNS session helper sniffs the return packet from an initial 1521 SQLNET exchange and then uses the port and session information uncovered in that return TNS redirect packet to add a temporary firewall policy that accepts the new port and IP address supplied as part of the TNS redirect.

The session helper configuration binds a session helper to a TCP or UDP port and protocol. When a session is accepted by a firewall policy on that port and protocol the FortiGate unit passes the session to the session helper configured with this command. The session is processed by the session helper.

If your FortiGate unit accepts sessions that require a session helper on different ports than those defined by the session-helper configuration, then you can add more entire to the session helper configuration. Its OK to have multiple session helper configurations for a given protocol because only the matching configuration is used.

Use the `show system session-helper` command to view the current session helper configuration.

FortiGate units include the session helpers listed in [Table 25](#):

Table 25: FortiGate session helpers

| Session helper name | Description |
|---------------------|--|
| dcerpc | Distributed computing environment / remote procedure calls protocol (DCE/RPC). |
| dns-tcp | Domain name service (DNS) using the TCP protocol. |
| dns-udp | Domain name service (DNS) using the UDP protocol. |
| ftp | File transfer protocol (FTP). |
| h245I | H.245 I call-in protocol. |
| h245O | H.256 O call-out protocol. |
| h323 | H.323 protocol. |
| mgcp | Media gateway control protocol (MGCP). |
| mms | Multimedia message service (MMS) protocol |
| pmap | Port mapper (PMAP) protocol. |
| pptp | Point to point tunneling protocol (PPTP). |

Table 25: FortiGate session helpers

| Session helper name | Description |
|---------------------|--|
| ras | Remote access service (RAS) protocol. |
| rsh | Remote shell protocol (RSH). |
| sip | Session initiation protocol (SIP). |
| tftp | Trivial file transfer protocol (TFTP). |
| tns | Oracle transparent network substrate protocol (TNS or SQLNET). |

Syntax

```

config system session-helper
  edit <helper-number>
    set name {dcerpc | dns-tcp | dns-udp | ftp | h245I | H2450
              | h323 | mgcp | mms | pmap | pptp | ras | rsh | sip | tftp
              | tns}
    set port <port_number>
    set protocol <protocol_number>
  end

```

| Variable | Description | Default |
|--|--|-------------|
| <helper-number> | Enter the number of the session-helper that you want to edit, or enter an unused number or 0 to create a new session-helper. | No default. |
| name {dcerpc dns-tcp dns-udp ftp h245I H2450 h323 mgcp mms pmap pptp ras rsh sip tftp tns} | The name of the session helper to configure. | No default. |
| port <port_number> | Enter the port number to use for this protocol. | No default. |
| protocol <protocol_number> | The protocol number for this service, as defined in RFC 1700 . | No default. |

session-sync

Use this command to configure TCP session synchronization between two standalone FortiGate units. You can use this feature with external routers or load balancers configured to distribute or load balance TCP sessions between two peer FortiGate units. If one of the peers fails, session failover occurs and active TCP sessions fail over to the peer that is still operating. This failover occurs without any loss of data. As well the external routers or load balancers will detect the failover and re-distribute all sessions to the peer that is still operating.



TCP session synchronization between two standalone FortiGate units is also sometimes called standalone session synchronization or session synchronization between non-HA FortiGate units.

You cannot configure standalone session synchronization when HA is enabled.

Syntax

```
config system session-sync
  edit <sync_id>
    set peerip <peer_ipv4>
    set peervd <vd_name>
    set syncvd <vd_name>
    config filter
      set dstaddr <dst_ip_ipv4> <dst_mask_ipv4>
      set dstaddr6 <dst_ip_ipv6>
      set dstintf <interface_name>
      set service <string>
      set srcaddr <src_ip_ipv4> <src_mask_ipv4>
      set srcaddr6 <src_ip_ipv6>
      set srcintf <interface_name>
      config custom-service
        edit <service_filter_id>
          set src-port-range <xxx-yyy>
          set dst-port-range <xxx-yyy>
        end
      end
    end
  end
end
```

| Variable | Description | Default |
|---------------------|--|-------------|
| <service_filter_id> | Enter the unique ID for the service filter. | |
| <sync_id> | Enter the unique ID number for the session synchronization configuration to edit. The session synchronization configuration ID can be any number between 1 and 200. The session synchronization configuration IDs of the peers do not have to match. | No default. |
| peerip <peer_ipv4> | Enter the IP address of the interface on the peer unit that is used for the session synchronization link. | 0.0.0.0 |

| Variable | Description | Default |
|--|--|--------------------------------|
| peervd <vd_name> | Enter the name of the virtual domain that contains the session synchronization link interface on the peer unit. Usually both peers would have the same <code>peervd</code> . Multiple session synchronization configurations can use the same <code>peervd</code> . | root |
| syncvd <vd_name> | Enter the names of one or more virtual domains so that the sessions processed by these virtual domains are synchronized using this session synchronization configuration. | |
| config custom-service | Add a service filter for session sync. | |
| config filter | Add a filter to a standalone session synchronization configuration. You can add a filter if you want to only synchronize some TCP sessions. Using a filter you can configure synchronization to only synchronize sessions according to source and destination address, source and destination interface, and predefined firewall TCP service. You can only add one filter to a standalone session synchronization configuration. | |
| dstaddr <dst_ip_ipv4> <dst_mask_ipv4> dstaddr6 <dst_ip_ipv6> | Enter the destination IP address (or range) and netmask of the sessions to synchronize. For IPv4 addresses, use <code>dstaddr</code> . For IPv6 addresses, use <code>dstaddr6</code> . The default IP address and netmask (0.0.0.0 / 0.0.0.0 or :: / 0) synchronizes sessions for all destination address. If you want to specify multiple IP addresses or address ranges you can add multiple standalone session synchronization configurations. | 0.0.0.0 0.0.0.0 ::/0 |
| dstintf <interface_name> | Enter the name of a FortiGate interface (this can be any interface including a VLAN interface, aggregate interface, redundant interface, virtual SSL VPN interface, or inter-VDOM link interface). Only sessions destined for this interface are synchronized. You can only enter one interface name. If you want to synchronize sessions for multiple interfaces you can add multiple standalone session synchronization configurations. The default <code>dstintf</code> setting synchronizes sessions for all interfaces. | (null) |
| dst-port-range <xxx-yyy> | Enter the destination port range for the service filter. | (null) |
| service <string> | Enter the name of a FortiGate firewall predefined service. Only sessions that use this predefined service are synchronized. You can only enter one predefined service name. If you want to synchronize sessions for multiple services you can add multiple standalone session synchronization configurations. | (null) |

| Variable | Description | Default |
|--|--|--------------------------------|
| srcaddr <src_ip_ipv4> <src_mask_ipv4> srcaddr6 <src_ip_ipv6> | Enter the source IP address and netmask of the sessions to synchronize. For IPv4 addresses, use <code>srcaddr</code> . For IPv6 addresses, use <code>srcaddr6</code> . The default IP address and netmask (0.0.0.0/0.0.0.0 or ::/0) synchronizes sessions for all source address. If you want to specify multiple IP addresses or address ranges you can add multiple standalone session synchronization configurations. | 0.0.0.0 0.0.0.0 ::/0 |
| srcintf <interface_name> | Enter the name of a FortiGate interface (this can be any interface including a VLAN interface, aggregate interface, redundant interface, virtual SSL VPN interface, or inter-VDOM link interface). Only sessions from this interface are synchronized. You can only enter one interface name. If you want to synchronize sessions for multiple interfaces you can add multiple standalone session synchronization configurations. The default <code>srcintf</code> setting synchronizes sessions for all interfaces. | (null) |
| src-port-range <xxx-yyy> | Enter the source port range for the service filter. | (null) |

session-ttl

Use this command to configure port-range based session timeouts by setting the session time to live (ttl) for multiple TCP, UDP, or SCTP port number ranges. The session ttl is the length of time a TCP, UDP, or SCTP session can be idle before being dropped by the FortiGate unit. You can add multiple port number ranges. For each range you can configure the protocol (TCP, UDP, or SCTP) and start and end numbers of the port number range.

Syntax

```
config system session-ttl
  set default <seconds>
  config port
    edit <entry_id>
      set end-port <port_number_int>
      set protocol <protocol_int>
      set start-port <port_number_int>
      set timeout {<timeout_int> | never}
    end
  end
```

| Variable | Description | Default |
|-------------------------------|--|-------------|
| default <seconds> | Enter the default session timeout in seconds. The valid range is from 300 - 604 800 seconds. This affects only TCP and SCTP sessions that do not have a timeout specified in a defined config port entry. | 3600 |
| <entry_id> | Enter an entry ID. Range 0-65535. This is just an identifier, and does not assign the port number. | No default. |
| end-port <port_number_int> | The end port number of the port number range. You must configure both the start-port and end-port. To specify a range, the start-port value must be lower than the end-port value. To specify a single port, the start-port value must be identical to the end-port value. The range is 0 to 65 535. | 0 |
| protocol <protocol_int> | Enter the protocol number to match the protocol of the sessions for which to configure a session ttl range. The Internet Protocol Number is found in the IP packet header. RFC 5237 describes protocol numbers and you can find a list of the assigned protocol numbers here . The range is from 0 to 255. To enter a port number range you must set protocol to 6 for TCP sessions, to 17 for UDP sessions, or to 132 for SCTP sessions. | 0 |

| Variable | Description | Default |
|------------------------------------|---|---------|
| start-port <port_number_int> | The start port number of the port number range. You must configure both the <code>start-port</code> and <code>end-port</code> . To specify a range, the <code>start-port</code> value must be lower than the <code>end-port</code> value. To specify a single port, the <code>start-port</code> value must be identical to the <code>end-port</code> value. The range is 0 to 65 535. | 0 |
| timeout {<timeout_int> never} | Enter the number of seconds the session can be idle for on this port. The valid range is from 1 - 604800 seconds. Optionally you can enter <code>never</code> instead of specifying the number of seconds if you want the session to never expire. Caution: While it is possible to set <code>timeout</code> to <code>never</code> , this is not a secure configuration and should be avoided. | 300 |

settings

Use this command to change settings that are per VDOM settings such as the operating mode and default gateway.

When changing the opmode of the VDOM, there are fields that are visible depending on which opmode you are changing to. They are only visible after you set the opmode and before you commit the changes with either 'end' or 'next'. If you do not set these fields, the opmode change will fail.

Table 26: Fields associated with each opmode

| Change from NAT to Transparent mode | Change from Transparent to NAT mode |
|--|--|
| <pre>set gateway <gw_ipv4></pre> <pre>set manageip <manage_ipv4></pre> | <pre>set device <interface_name></pre> <pre>set gateway <gw_ipv4></pre> <pre>set ip <address_ipv4></pre> |

`system settings` differs from `system global` in that `system global` fields apply to the entire FortiGate unit, where `system settings` fields apply only to the current VDOM, or the entire FortiGate unit if VDOMs are not enabled.

Bi-directional Forwarding Detection (BFD) is a protocol used by BGP and OSPF. It is used to quickly locate hardware failures in the network. Routers running BFD communicate with each other, and if a timer runs out on a connection then that router is declared down. BFD then communicates this information to the routing protocol and the routing information is updated. BFD support was added in FortiOS v3.0 MR4, and can only be configured through the CLI.



When asymmetric routing is enabled, through the use of `asymroute` field, the FortiGate unit can no longer perform stateful inspection.

Syntax

```
config system settings
  set allow-subnet-overlap {enable | disable}
  set asymroute {enable | disable}
  set asymroute6 {enable | disable}
  set bfd {enable | disable}
  set bfd-desired-min-tx <interval_msec>
  set bfd-required-min-rx <interval_msec>
  set bfd-detect-mult <multiplier>
  set bfd-dont-enforce-src-port {enable | disable}
  set deny-tcp-with-icmp {enable | disable}
  set device <interface_name>
  set discovered-device-timeout <days_int>
  set ecmp-max-paths <max_entries>
  set firewall-session-dirty {check-all | check-new
    | check-policy-option}
  set gateway <gw_ipv4>
  set gateway6 <gw_ipv6>
```

```

set gui-default-policy-columns <column_list>
set ip <address_ipv4>
set ip6 <address_ipv6>
set mac-ttl <seconds_int>
set manageip <manage_ipv4>
set manageip6 <manage_ipv6>
set multicast-forward {enable | disable}
set multicast-skip-policy {enable | disable}
set multicast-ttl-notchange {enable | disable}
set opmode {nat | transparent}
set per-ip-bandwidth {enable | disable}
set sccp-port <port_number>
set ses-denied-traffic {enable | disable}
set sip-helper {enable | disable}
set sip-nat-trace {enable | disable}
set sip-ssl-port <port_number>
set sip-tcp-port <port1_int> [<port2_int>]>
set sip-udp-port <port_number>
set status {enable | disable}
set strict-src-check {enable | disable}
set utf8-spam-tagging {enable | disable}
set v4-ecmp-mode {source-ip-based | usage-based | weight-based}
set vpn-stats-log {ipsec | l2tp | pptp | ssl}
set vpn-stats-period <period_int>
set wccp-cache-engine {enable | disable}
end

```

| Variable | Description | Default |
|--|---|---------|
| allow-subnet-overlap {enable disable} | <p>Enable limited support for interface and VLAN subinterface IP address overlap for this VDOM. Use this command to enable limited support for overlapping IP addresses in an existing network configuration.</p> <p>Caution: for advanced users only. Use this only for existing network configurations that cannot be changed to eliminate IP address overlapping.</p> | disable |
| asymroute {enable disable} | <p>Enable to turn on IPv4 asymmetric routing on your FortiGate unit, or this VDOM if you have VDOMs enabled.</p> <p>This feature should only be used as a temporary check to troubleshoot a network. It is not intended to be enabled permanently. When it enabled, many security features of your FortiGate unit are not enabled.</p> <p>Note: Enabling asymmetric routing disables stateful inspection. Your FortiGate unit can only perform stateless inspection in this state.</p> | disable |
| asymroute6 {enable disable} | <p>Enable to turn on IPv6 asymmetric routing on your FortiGate unit, or this VDOM if you have VDOMs enabled.</p> | disable |

| Variable | Description | Default |
|---|---|-------------|
| bfd {enable disable} | Enable to turn on bi-directional forwarding detection (BFD) for this virtual domain, or the whole FortiGate unit. BFD can be used with OSPF and BGP configurations, and overridden on a per interface basis. | disable |
| bfd-desired-min-tx <interval_msec> | Enter a value from 1 to 100 000 msec as the preferred minimum transmit interval for BFD packets. If possible this will be the minimum used. This variable is only available when bfd is enabled. | 50 |
| bfd-required-min-rx <interval_msec> | Enter a value from 1 to 100 000 msec as the required minimum receive interval for BFD packets. The FortiGate unit will not transmit BFD packets at a slower rate than this. This variable is only available when bfd is enabled. | 50 |
| bfd-detect-mult <multiplier> | Enter a value from 1 to 50 for the BFD detection multiplier. | 3 |
| bfd-dont-enforce-src-port {enable disable} | Enable to not enforce the BFD source port. | disable |
| deny-tcp-with-icmp {enable disable} | Enable to deny TCP by sending an ICMP Communication Prohibited packet. Firewall policies will enable send-deny-packet. | disable |
| device <interface_name> | Enter the interface to use for management access. This is the interface to which ip applies. This field is visible only after you change opmode from transparent to nat, before you commit the change. | No default. |
| discovered-device-timeout <days_int> | Enter the timeout for discovered devices. Range: 1 to 365 days. | 28 |
| ecmp-max-paths <max_entries> | Enter the maximum number of routes allowed to be included in an Equal Cost Multi-Path (ECMP) configuration. Set to 1 to disable ECMP routing. ECMP routes have the same distance and the same priority, and can be used in load balancing. | 10 |
| email-portal-check-dns {enable disable} | Enable to have the email collection portal verify that the domain name part of email address can be resolved using a DNS lookup. | enable |

| Variable | Description | Default |
|--|---|-------------|
| firewall-session-dirty { check-all check-new check-policy-option } | Select how to manage changes to a firewall policy: check-all — flush all current sessions and re-evaluate them check-new — keep existing sessions and apply policy change to new sessions only. This reduces CPU load and the possibility of packet loss. check-policy-option — use the option selected in the firewall-session-dirty field of the firewall policy. See “firewall policy, policy6” on page 167 . | check-all |
| gateway <gw_ipv4> | Enter the default gateway IP address. This field is visible only after you change <code>opmode</code> from <code>nat</code> to <code>transparent</code> or from <code>transparent</code> to <code>nat</code> , before you commit the change. | No default. |
| gateway6 <gw_ipv6> | Enter the default gateway IPv6 address. This field is visible only after you change <code>opmode</code> from <code>nat</code> to <code>transparent</code> or from <code>transparent</code> to <code>nat</code> , before you commit the change. | No default. |
| gui-default-policy-columns <column_list> | Optionally, override the web-based manager's default displayed column set for firewall policies. <code><column_list></code> is a space-delimited list containing any of the following column names in the desired order of appearance from left to right: <code>#</code> , <code>policyid</code> , <code>srcintf</code> , <code>dstintf</code> , <code>srcaddr</code> , <code>dstaddr</code> , <code>schedule</code> , <code>service</code> , <code>action</code> , <code>logtraffic</code> , <code>nat</code> , <code>status</code> , <code>authentication</code> , <code>count</code> , <code>profile</code> , <code>vpntunnel</code> , <code>comments</code> | (null) |
| ip <address_ipv4> | Enter the IP address to use after switching to <code>nat</code> mode. This field is visible only after you change <code>opmode</code> from <code>transparent</code> to <code>nat</code> , before you commit the change. | No default. |
| ip6 <address_ipv6> | Enter the IPv6 address to use after switching to <code>nat</code> mode. This field is visible only after you change <code>opmode</code> from <code>transparent</code> to <code>nat</code> , before you commit the change. | No default. |
| mac-ttl <seconds_int> | Set duration of MAC addresses during transparent mode. Range: 300 to 8 640 000 seconds (100days). | 300 |
| manageip <manage_ipv4> | Set the IP address and netmask of the Transparent mode management interface. You must set this when you change <code>opmode</code> from <code>nat</code> to <code>transparent</code> . | No default. |
| manageip6 <manage_ipv6> | Set the IPv6 management address prefix for Transparent mode. | No default. |

| Variable | Description | Default |
|---|--|-------------|
| multicast-forward { enable disable } | Enable or disable multicast forwarding to forward any multicast IP packets in which the TTL is 2 or higher to all interfaces and VLAN interfaces except the receiving interface. The TTL in the IP header will be reduced by 1. When multiple VDOMs are configured, this option is available within each VDOM. | enable |
| multicast-skip-policy { enable disable } | Must be disabled when using multicast security policies. This field is visible only after you change <code>opmode</code> from <code>nat</code> to <code>transparent</code> , before you commit the change. | No default. |
| multicast-ttl-notchange { enable disable } | Enable to alter multicast forwarding so that it does not decrement the time-to-live (TTL) in the packet header. Disable for normal multicast forwarding behavior. In multiple VDOM mode, this option is only available within VDOMs. It is not available at the global level. | disable |
| opmode { nat transparent } | Enter the required operating mode. If you change <code>opmode</code> from <code>nat</code> to <code>transparent</code> , you must set <code>manageip</code> and <code>gateway</code> . If you change <code>opmode</code> from <code>transparent</code> to <code>nat</code> , you must set <code>device</code> , <code>ip</code> , <code>gateway-device</code> and <code>gateway</code> . | nat |
| per-ip-bandwidth { enable disable } | Enable or disable per-IP bandwidth reporting. | enable |
| sccp-port <port_number> | Enter the port number from 1 to 65535 of the TCP port to use to monitor Skinny Client Call protocol (SCCP) traffic. SCCP is a Cisco proprietary protocol for VoIP. | 2000 |
| ses-denied-traffic { enable disable } | Enable or disable including denied traffic in session table. | disable |
| sip-helper { enable disable } | Enable or disable the SIP session helper. The SIP session helper will process SIP sessions unless the SIP sessions are accepted by the SIP ALG. | enable |
| sip-nat-trace { enable disable } | Select enable to record the original IP address of the phone. | enable |
| sip-ssl-port <port_number> | Enter the port number from 1 to 65535 that the SIP proxy monitors for SIP traffic. | 5061 |
| sip-tcp-port <port1_int> [<port2_int>]> | Enter of one or two port numbers (range 1 to 65535) that the SIP ALG monitors for SIP TCP sessions. | 5060 |
| sip-udp-port <port_number> | Enter the port number from 1 to 65535 that the SIP ALG monitors for SIP UDP sessions. | 5060 |

| Variable | Description | Default |
|---|--|-----------------|
| status {enable disable} | <p>Disable or enable this VDOM. Disabled VDOMs keep all their configuration, but the resources of that VDOM are not accessible.</p> <p>To leave VDOM mode, all disabled VDOMs must be deleted - to leave VDOM mode there can be only the root VDOM configured.</p> <p>Only available when VDOMs are enabled.</p> | enable |
| strict-src-check {enable disable} | Enable to refuse packets from a source IP range if there is a specific route in the routing table for this network (RFC 3704). | disable |
| utf8-spam-tagging {enable disable} | Enable converts spam tags to UTF8 for better non-ascii character support. | enable |
| v4-ecmp-mode {source-ip-based usage-based weight-based} | <p>Set the ECMP route failover and load balance method, which controls how the FortiGate unit assigns a route to a session when multiple equal-cost routes to the sessions's destination are available. You can select:</p> <p>source-ip-based — the FortiGate unit load balances sessions among ECMP routes based on the source IP address of the sessions to be load balanced. No other settings can be configured to support source IP load balancing.</p> <p>weight-based — the FortiGate unit load balances sessions among ECMP routes based on weights added to ECMP routes. More traffic is directed to routes with higher weights. Use the <code>weight</code> field of the <code>config router static</code> command to add weights to static routes. See “router static” on page 446.</p> <p>usage-based — the FortiGate unit distributes sessions among ECMP routes based on how busy the FortiGate interfaces added to the routes are. After selecting <code>usage-based</code> you use the <code>spillover-threshold</code> field of the <code>config system interface</code> command to add spillover thresholds to interfaces added to ECMP routes. The FortiGate unit sends all ECMP-routed sessions to the lowest numbered interface until the bandwidth being processed by this interface reaches its spillover threshold. The FortiGate unit then spills additional sessions over to the next lowest numbered interface. See “system interface” on page 555.</p> | source-ip-based |
| vpn-stats-log {ipsec l2tp pptp ssl} | Enable periodic VPN log statistics for one or more types of VPN. | |

| Variable | Description | Default |
|---|--|---------|
| vpn-stats-period <period_int> | Enter the interval in seconds for <code>vpn-stats-log</code> to collect statistics. | 0 |
| wccp-cache-engine {enable disable} | Configure the FortiGate unit to operate as a WCCP cache engine. Use the <code>config system wccp</code> command to configure WCCP cache engine settings. | disable |

sit-tunnel

Use this command to tunnel IPv6 traffic over an IPv4 network. The IPv6 interface is configured under `config system interface`. The command to do the reverse is `system ipv6-tunnel`. This command is not available in Transparent mode.

Syntax

```
config system sit-tunnel
  edit <tunnel_name>
    set destination <tunnel_address>
    set interface <name>
    set ip6 <address_ipv6>
    set source <address_ipv4>
  end
```

| Variable | Description | Default |
|------------------------------|---|-------------|
| edit <tunnel_name> | Enter a name for the IPv6 tunnel. | No default. |
| destination <tunnel_address> | The destination IPv4 address for this tunnel. | 0.0.0.0 |
| interface <name> | The interface used to send and receive traffic for this tunnel. | No default. |
| ip6 <address_ipv6> | The IPv6 address for this tunnel. | No default. |
| source <address_ipv4> | The source IPv4 address for this tunnel. | 0.0.0.0 |

sflow

Use this command to add or change the IP address and UDP port that FortiGate sFlow agents use to send sFlow datagrams to an sFlow collector.

sFlow is a network monitoring protocol described in <http://www.sflow.org>. FortiOS implements sFlow version 5. You can configure one or more FortiGate interfaces as sFlow agents that monitor network traffic and send sFlow datagrams containing information about traffic flow to an sFlow collector.

sFlow is normally used to provide an overall traffic flow picture of your network. You would usually operate sFlow agents on switches, routers, and firewall on your network, collect traffic data from all of them and use a collector to show traffic flows and patterns.

Syntax

```
config system sflow
    set collector-ip <collector_ipv4>
    set collector_port <port_int>
    set source-ip <ipv4_addr>
end
```

| Variable | Description | Default |
|----------------------------------|--|---------|
| collector-ip <collector_ipv4> | The IP address of the sFlow collector that sFlow agents should send sFlow datagrams to. | 0.0.0.0 |
| collector_port <port_int> | The UDP port number used for sending sFlow datagrams. Change this setting only if required by your sFlow collector or you network configuration. | 6343 |
| source-ip <ipv4_addr> | Enter the source IP address for the sFlow agent. | 0.0.0.0 |

sms-server

Use this command to configure cellphone service provider entries for use with the SMS text message option for two-factor authentication.

One option for two-factor authentication sends a token via SMS text message to a cell phone number when the user or admin attempts to log on to the FortiGate unit. This token must be entered for the user or admin to be authenticated and allowed access.

Syntax

```
config system sms-server
  edit <provider>
    set mail-server <server_name>
  end
```

| Variable | Description | Default |
|---------------------------|--|---------|
| edit <provider> | Enter the name of a cell phone service provider. Maximum length allowed is 32 characters. To enter a name that includes spaces enclose the name in quotes. | null |
| mail-server <server_name> | Enter the address of the mail server that will accept the email and forward the message to the destination cell phone as an SMS text message. | null |

snmp community

Use this command to configure SNMP communities on your FortiGate unit. You add SNMP communities so that SNMP managers can connect to the FortiGate unit to view system information and receive SNMP traps. SNMP traps are triggered when system events happen such as when antivirus checking is bypassed, or when the log disk is almost full.

You can add up to three SNMP communities. Each community can have a different configuration for SNMP queries and traps. Each community can be configured to monitor the FortiGate unit for a different set of events. You can also add IP addresses of up to 8 SNMP managers to each community.



Part of configuring an SNMP manager is to list it as a host in a community on the FortiGate unit it will be monitoring. Otherwise the SNMP monitor will not receive any traps from that FortiGate unit, or be able to query it.

Syntax

```
config system snmp community
  edit <index_number>
    set events <events_list>
    set name <community_name>
    set query-v1-port <port_number>
    set query-v1-status {enable | disable}
    set query-v2c-port <port_number>
    set query-v2c-status {enable | disable}
    set status {enable | disable}
    set trap-v1-lport <port_number>
    set trap-v1-rport <port_number>
    set trap-v1-status {enable | disable}
    set trap-v2c-lport <port_number>
    set trap-v2c-rport <port_number>
    set trap-v2c-status {enable | disable}
  config hosts
    edit <host_number>
      set elbc-management {enable | disable}
      set ha-direct {enable | disable}
      set host-type {any | query | trap}
      set interface <if_name>
      set ip <address_ipv4>
      set source-ip <address_ipv4/mask>
    end
  config hosts6
    edit <host_number>
      set ha-direct {enable | disable}
      set interface <if_name>
      set ip6 <address_ipv6>
      set source-ip6 <address_ipv6>
    end
end
```


end

| Variable | Description | Default |
|------------------------|--|---------------------|
| edit <index_number> | Enter the index number of the community in the SNMP communities table. Enter an unused index number to create a new SNMP community. | |
| events <events_list> | <p>Enable the events for which the FortiGate unit should send traps to the SNMP managers in this community.</p> <p>av-bypass — FortiGate unit has entered bypass mode.</p> <p>See “set av-failopen pass” under “global” on page 523.</p> <p>av-conserve — System enters conserve mode.</p> <p>av-fragmented — A fragmented file has been detected.</p> <p>av-oversize — An oversized file has been detected.</p> <p>av-oversize-blocked — An oversized file has been blocked.</p> <p>av-oversize-passed — An oversized file has passed through.</p> <p>av-pattern — An file matching the AV pattern is detected.</p> <p>av-virus — A virus is detected.</p> <p>bgp-backward-transition — BGP FSM from a high-numbered to a low-numbered state.</p> <p>bgp-established — BGP FSM enters the established state.</p> <p>cpu-high — CPU usage exceeds threshold. Default is 80%. Automatic smoothing ensures only prolonged high CPU usage will trigger this trap, not a momentary spike.</p> <p>ent-conf-change — entity config change (rfc4133)</p> <p>fan-failure — A cooling fan has failed.</p> <p>faz-disconnect — A FortiAnalyzer device has disconnected from the FortiGate unit.</p> <p>fm-conf-change — FortiGate unit is managed by FortiManager, but the FortiGate administrator has modified the configuration directly.</p> <p>fm-if-change — FortiManager interface changes.</p> <p>ha-hb-failure — The HA heartbeat interface has failed.</p> <p>ha-member-down — The HA cluster member stops.</p> <p>ha-member-up — The HA cluster members starts.</p> <p>ha-switch — The primary unit in a HA cluster fails and is replaced with a new HA unit.</p> <p>intf-ip — The IP address of a FortiGate interface changes.</p> <p>ips-anomaly — IPS detects an anomaly.</p> <p>ips-fail-open — IPS network buffer is full.</p> <p>ips-pkg-update — IPS package has been updated.</p> <p>ips-signature — IPS detects an attack.</p> | All events enabled. |

| Variable | Description | Default |
|--|--|-------------|
| | load-balance-real-server-down — real server is down. log-full — Hard drive usage exceeds threshold. Default is 90%. mem-low — Memory usage exceeds threshold. Default is 80%. power-supply-failure — Power outage detected on monitored power supply. Available only on some models. vpn-tun-down — A VPN tunnel stops. vpn-tun-up — A VPN tunnel starts. | |
| name <community_name> | Enter the name of the SNMP community. | No default. |
| query-v1-port <port_number> | Enter the SNMP v1 query port number used for SNMP manager queries. | 161 |
| query-v1-status {enable disable} | Enable or disable SNMP v1 queries for this SNMP community. | enable |
| query-v2c-port <port_number> | Enter the SNMP v2c query port number used for SNMP manager queries. | 161 |
| query-v2c-status {enable disable} | Enable or disable SNMP v2c queries for this SNMP community. | enable |
| status {enable disable} | Enable or disable the SNMP community. | enable |
| trap-v1-lport <port_number> | Enter the SNMP v1 local port number used for sending traps to the SNMP managers. | 162 |
| trap-v1-rport <port_number> | Enter the SNMP v1 remote port number used for sending traps to the SNMP managers. | 162 |
| trap-v1-status {enable disable} | Enable or disable SNMP v1 traps for this SNMP community. | enable |
| trap-v2c-lport <port_number> | Enter the SNMP v2c local port number used for sending traps to the SNMP managers. | 162 |
| trap-v2c-rport <port_number> | Enter the SNMP v2c remote port number used for sending traps to the SNMP managers. | 162 |
| trap-v2c-status {enable disable} | Enable or disable SNMP v2c traps for this SNMP community. | enable |
| hosts, hosts6 variables | | |
| edit <host_number> | Enter the index number of the host in the table. Enter an unused index number to create a new host. | |
| elbc-management {enable disable} | Enable to allow use of snmp over the base channel and front panel ports in ELBC mode. | |
| ha-direct {enable disable} | Enable direct management of cluster members. | disable |
| host-type {any query trap} | Set permitted actions for this host: query—make queries only trap—receive traps only any—any SMTP action | any |

| Variable | Description | Default |
|--------------------------------------|--|---------------------|
| interface <if_name> | Enter the name of the FortiGate interface to which the SNMP manager connects. | No default. |
| ip <address_ipv4> | Enter the IPv4 IP address of the SNMP manager (for <code>hosts</code>). | 0.0.0.0 |
| ip6 <address_ipv6> | Enter the IPv6 IP address of the SNMP manager (for <code>hosts6</code>). | :: |
| source-ip <address_ipv4/mask > | Enter the source IPv4 IP address for SNMP traps sent by the FortiGate unit (for <code>hosts</code>). | 0.0.0.0/ 0.0.0.0 |
| source-ip6 <address_ipv6> | Enter the source IPv6 IP address for SNMP traps sent by the FortiGate unit (for <code>hosts6</code>). | :: |

snmp sysinfo

Use this command to enable the FortiGate SNMP agent and to enter basic system information used by the SNMP agent. Enter information about the FortiGate unit to identify it. When your SNMP manager receives traps from the FortiGate unit, you will know which unit sent the information. Some SNMP traps indicate high CPU usage, log full, or low memory.

Syntax

```
config system snmp sysinfo
    set contact-info <info_str>
    set description <description>
    set engine-id <engine-id_str>
    set location <location>
    set status {enable | disable}
    set trap-high-cpu-threshold <percentage>
    set trap-log-full-threshold <percentage>
    set trap-low-memory-threshold <percentage>
end
```

| Variable | Description | Default |
|--------------------------------------|---|-------------|
| contact-info <info_str> | Add the contact information for the person responsible for this FortiGate unit. The contact information can be up to 35 characters long. | No default. |
| description <description> | Add a name or description of the FortiGate unit. The description can be up to 35 characters long. | No default. |
| engine-id <engine-id_str> | Each SNMP engine maintains a value, snmpEngineID, which uniquely identifies the SNMP engine. This value is included in each message sent to or from the SNMP engine. In FortiOS, the snmpEngineID is composed of two parts: <ul style="list-style-type: none"> Fortinet prefix 0x8000304404 the optional engine-id string, 24 characters maximum, defined in this command Optionally, enter an engine-id value. | No default. |
| location <location> | Describe the physical location of the FortiGate unit. The system location description can be up to 35 characters long. Note: XSS vulnerability checking is disabled, so XSS characters such as '(' and ')' are permitted. | No default. |
| status {enable disable} | Enable or disable the FortiGate SNMP agent. | disable |
| trap-high-cpu-threshold <percentage> | Enter the percentage of CPU used that will trigger the threshold SNMP trap for the high-cpu. There is some smoothing of the high CPU trap to ensure the CPU usage is constant rather than a momentary spike. This feature prevents frequent and unnecessary traps. | 80 |

| Variable | Description | Default |
|---|---|---------|
| trap-log-full-threshold <percentage> | Enter the percentage of disk space used that will trigger the threshold SNMP trap for the log-full. | 90 |
| trap-low-memory-threshold <percentage> | Enter the percentage of memory used that will be the threshold SNMP trap for the low-memory. | 80 |

snmp user

Use this command to configure an SNMP user including which SNMP events the user wants to be notified about, which hosts will be notified, and if queries are enabled which port to listen on for them.

FortiOS implements the user security model of RFC 3414. You can require the user to authenticate with a password and you can use encryption to protect the communication with the user.

Syntax

```
config system snmp user
  edit <username>
    set auth-proto {md5 | sha}
    set auth-pwd <password>
    set events <event_string>
    set ha-direct {enable | disable}
    set notify-hosts <hosts_string>
    set notify-hosts6 <hosts_string>
    set priv-proto {aes | des}
    set priv-pwd <key>
    set queries {enable | disable}
    set query-port <port_int>
    set security-level <slevel>
  end
```

| Variable | Description | Default |
|---------------------------|---|-------------|
| edit <username> | Edit or add selected user. | No default. |
| auth-proto {md5 sha} | Select authentication protocol: md5 — use HMAC-MD5-96 authentication protocol. sha — use HMAC-SHA-96 authentication protocol. This is only available if security-level is auth-priv or auth-no-priv. | sha |
| auth-pwd <password> | Enter the user’s password. Maximum 32 characters. This is only available if security-level is auth-priv or auth-no-priv. | No default. |

| Variable | Description | Default |
|---------------------------------|--|-------------|
| events <event_string> | <p>Select which SNMP notifications to send. Select each event that will generate a notification, and add to string. Separate multiple events by a space. Available events include:</p> <p>amc-bypass — an AMC bridge module has switched to bridge (bypass) mode.</p> <p>av-bypass — AV bypass happens</p> <p>av-conserve — AV system enters conserve mode</p> <p>av-fragmented — AV detected fragmented file</p> <p>av-oversize — AV detected oversized file</p> <p>av-oversize-blocked — AV oversized files blocked</p> <p>av-oversize-passed — AV oversized files passed</p> <p>av-pattern — AV detected file matching pattern</p> <p>av-virus — AV detected virus</p> <p>cpu-high — cpu usage too high</p> <p>ent-conf-change — entity config change (rfc4133)</p> <p>fan-failure — A cooling fan has failed.</p> <p>faz-disconnect — FortiAnalyzer unit disconnected</p> <p>fm-conf-change — config change (FM trap)</p> <p>fm-if-change — interface IP change (FM trap)</p> <p>ha-hb-failure — HA heartbeat interface failure</p> <p>ha-member-down — HA cluster member down</p> <p>ha-member-up — HA cluster member up</p> <p>ha-switch — HA cluster status change</p> <p>intf-ip — interface IP address changed</p> <p>ips-anomaly — ips detected an anomaly</p> <p>ips-pkg-update — ips package updated</p> <p>ips-signature — ips detected an attack</p> <p>log-full — available log space is low</p> <p>mem-low — available memory is low</p> <p>power-supply-failure — power supply failure</p> <p>vpn-tun-down — VPN tunnel is down</p> <p>vpn-tun-up — VPN tunnel is up</p> <p>Note: On the <code>events</code> field, the <code>unset</code> command clears all options.</p> | No default. |
| ha-direct {enable disable} | Enable direct management of cluster members. | disable |
| notify-hosts <hosts_string> | Enter IPv4 IP addresses to send SNMP notifications (SNMP traps) to when events occur. Separate multiple addresses with a space. | No default. |

| Variable | Description | Default |
|---------------------------------|--|-----------------|
| notify-hosts6 <hosts_string> | Enter IPv6 IP addresses to send SNMP notifications (SNMP traps) to when events occur. Separate multiple addresses with a space. | No default. |
| priv-prot {aes des} | Select privacy (encryption) protocol: aes — use CFB128-AES-128 symmetric encryption. des — use CBC-DES symmetric encryption. This is available if <code>security-level</code> is <code>auth-priv</code> . | aes |
| priv-pwd <key> | Enter the privacy encryption key. Maximum 32 characters. This is available if <code>security-level</code> is <code>auth-priv</code> . | No default. |
| queries {enable disable} | Enable or disable SNMP v3 queries for this user. Queries are used to determine the status of SNMP variables. | enable |
| query-port <port_int> | Enter the number of the port used for SNMP v3 queries. If multiple versions of SNMP are being supported, each version should listen on a different port. | 161 |
| security-level <slevel> | Set security level to one of: no-auth-no-priv — no authentication or privacy auth-no-priv — authentication but no privacy auth-priv — authentication and privacy | no-auth-no-priv |

sp

Use this command to configure offloading traffic to a FortiASIC Security Processing (SP) Module. Fortinet security processing modules provide multi-gigabit throughput increases for intrusion prevention, firewall, and IP multicast applications. All models are based on the carrier-class Advanced Mezzanine Card™ (AMC) specification.

FortiGate units that support these modules offer a third action. Legitimate connections are allowed while an attack is blocked.

This command is only available on models with one or more AMC slots and a FortiASIC Security Processing Module installed. When VDOMs are enabled, this is a global command.

Syntax

```
config system sp
  set name <string>
  set ips-weight {less-fw | balanced | all-ips}
  set fp-disable {all | ips | ipsec | multicast | DoS | none}
  set ipsec-inb-optimization {enable | disable}
  set syn-proxy-client-timer <sec_int>
  set syn-proxy-server-timer <sec_int>
end
```

| Variable | Description | Default |
|---|---|---------|
| name <string> | Maximum of 31 characters. | |
| ips-weight {less-fw balanced all-ips} | Select the weighting method for IPS sessions. Default is less-fw. <ul style="list-style-type: none"> less-fw balanced all-ips | less-fw |
| fp-disable {all ips ipsec multicast DoS none} | Select one or more types of traffic to exclude from file processing. Security processing modules can accelerate different security features such as firewall, IPS, multicast, and DoS. By default the modules will accelerate all those types of traffic, but you can disable acceleration of one or more of those types of traffic with this command. Any one or more types of traffic listed will not be accelerated, and will be handled by the FortiOS system. | none |
| ipsec-inb-optimization {enable disable} | Select to enable inbound IPsec optimization. | enable |

| Variable | Description | Default |
|-------------------------------------|---|---------|
| syn-proxy-client-timer <sec_int> | <p>Set the number of seconds for the client side timer for the three-way handshake. If the timer expires and the handshake is not complete, the connection is discarded. Range is 1 to 255. Default is 3.</p> <p>For the tcp_syn_flood threshold, in addition to Block and Pass, you can choose to Proxy connect attempts when their volume exceeds the threshold value. When the tcp_syn_flood threshold action is set to Proxy, incomplete TCP connections are allowed as normal as long as the configured threshold is not exceeded. If the threshold is exceeded, the FortiGate unit will intercept incoming SYN packets with a hardware accelerated SYN proxy to determine whether the connection attempts are legitimate or a SYN flood attack.</p> | 3 |
| syn-proxy-server-timer <sec_int> | <p>Set the number of seconds for the server side timer for the three-way handshake. If the timer expires and the handshake is not complete, the connection is discarded. Range is 1 to 255. Default is 3.</p> | 3 |

storage

Use this command to add and edit local disk storage settings.

Syntax

```
config system storage
  edit <storage_name>
    set media-type <name>
    set partition <partition_ref_int>
  end
```

| Variable | Description | Default |
|----------------------------------|--|---------|
| <storage_name> | The name for this storage. | |
| media-type <name> | The type of disk. You cannot configure or change this setting. | |
| partition <partition_ref_int> | The partition reference number. See “execute disk” on page 921 . | |

stp

Use this command to configure Spanning Tree Protocol on an Internal interface switch in switch mode.

Syntax

```
config system stp
  set config-revision <int>
  set forward-delay <secs_int>
  set hello-time <secs_int>
  set max-age <secs_int>
  set max-hops <hops_int>
  set region-name <name_str>
  set status {enable | disable}
  set switch-priority <prio_int>
end
```

| Variable | Description | Default |
|----------------------------|---|---------|
| config-revision <int> | Set the configuration revision. Range 0-65535. | 0 |
| forward-delay <secs_int> | Set forwarding delay. Range 4 to 30. | 15 |
| hello-time <secs_int> | Set hello time. Range 1 to 10. | 2 |
| max-age <secs_int> | Set maximum packet age. Range 6 to 40. | 20 |
| max-hops <hops_int> | Set maximum number of hops. Range 1 to 40. | 20 |
| region-name <name_str> | Set region name. | null |
| status {enable disable} | Enable or disable STP. | enable |
| switch-priority <prio_int> | Set priority. Permitted values: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, 61440. | 32768 |

switch-interface

Use this command to group physical and wifi interfaces into a software switch interface (also called a softswitch, soft-switch or soft switch). A software switch is a virtual switch that is implemented in software instead of hardware. When you add interfaces to a software switch the interfaces all share one IP address and become a single entry on the interface list. As a result, all of the interfaces are on the same subnet and traffic between devices connected to each interface of the software switch cannot be filtered by firewall policies.

Adding a software switch can be used to simplify communication between devices connected to different FortiGate interfaces. For example, using a software switch you can place the FortiGate interface connected to an internal network on the same subnet as your wireless interfaces. Then devices on the internal network can communicate with devices on the wireless network without any additional configuration on the FortiGate unit.

The physical and WiFi interfaces added to a software switch interface cannot be used in any other configurations. The wifi interfaces can be implemented on the FortiWiFi unit or on remote FortiWiFi units of FortiAP units controlled by the wireless controller feature. Interfaces in a software switch cannot be monitored by HA or used as heart beat devices.

This command can be used at the Global or VDOM level.

Syntax

```
config system switch-interface
  edit <group_name>
    set member <iflist>
    set span {enable | disable}
    set span-dest-port <portnum>
    set span-direction {rx | tx | both}
    set span-source-port <portlist>
    set type {hub | switch | hardware-switch}
    set vdom <vdom_name>
  end
```

| Variable | Description | Default |
|-----------------------------|---|-------------|
| <group_name> | The name for this software switch. Cannot be in use by any other interfaces, vlans, or inter-VDOM links. | No default. |
| member <iflist> | Enter a list of the interfaces that will be part of this software switch. Separate interface names with a space. Use <tab> to advance through the list of available interfaces. | No default. |
| span {enable disable} | Enable or disable port spanning. This is available only when <code>type</code> is <code>switch</code> . Port spanning echoes traffic received by the software switch to the span destination port. Port spanning can be used to monitor all traffic passing through the soft switch. You can also configure the span destination port and the span source ports., which are the switch ports for which traffic is echoed. | disable |
| span-dest-port <portnum> | Enter the span port destination port name. All traffic on the span source ports is echoed to the span destination port. Use <tab> to advance through the list of available interfaces. Available when <code>span</code> is enabled. | No default. |

| Variable | Description | Default |
|--|--|-------------|
| span-direction {rx tx both} | <p>Select the direction in which the span port operates:</p> <p>rx — Copy only received packets from source SPAN ports to the destination SPAN port.</p> <p>tx — Copy only transmitted packets from source SPAN ports to the destination SPAN port.</p> <p>both — Copy both transmitted and received packets from source SPAN ports to the destination SPAN port.</p> <p>span-direction is available only when span is enabled.</p> | both |
| span-source-port <portlist> | <p>Enter a list of the interfaces that are span source ports. Separate interface names with a space. Port spanning echoes all traffic on the span source ports to the span destination port.</p> <p>Use <tab> to advance through the list of available interfaces.</p> <p>Available when span is enabled.</p> | No default. |
| type {hub switch hardware-switch} | <p>Select the type of switch functionality:</p> <p>hub — duplicates packets to all member ports</p> <p>switch — normal switch functionality (available in NAT mode only)</p> | switch |
| vdom <vdom_name> | Enter the VDOM to which the software switch belongs. | No default. |

tos-based-priority

Use this command to prioritize your network traffic based on its type-of-service (TOS).

IP datagrams have a TOS byte in the header (as described in RFC 791). Four bits within this field determine the delay, the throughput, the reliability, and cost (as described in RFC 1349) associated with that service. There are 4 other bits that are seldom used or reserved that are not included here. Together these bits are the tos variable of the tos-based-priority command.

The TOS information can be used to manage network traffic and its quality based on the needs of the application or service. TOS application routing (RFC 1583) is supported by OSPF routing.

For more information on TOS in routing, see [“policy, policy6” on page 417](#).

Syntax

```
config system tos-based-priority
  edit <name>
    set tos <ip_tos_value>
    set priority [high | medium | low]
  end
```

| Variable | Description | Default |
|-----------------------------------|---|-------------|
| edit <name> | Enter the name of the link object to create | No default. |
| tos <ip_tos_value> | Enter the value of the type of service byte in the IP datagram header: 8 -- minimize delay 4 -- maximize throughput 2 -- maximize reliability 1 -- minimize monetary cost 0 -- default service | 0 |
| priority [high medium low] | Select the priority of this type of service as either high, medium, or low priority. These priority levels conform to the firewall traffic shaping priorities. | medium |

vdom-dns

Use this command to configure DNS servers for a non-management VDOM. This command is only available from a non-management VDOM

DNS settings such as `dns-cache-limit` and `set` globally. See “[system dns](#)” on page 508.

Syntax

```
config system vdom-dns
  set ip6-primary <dns_ipv6>
  set ip6-secondary <dns_ip6>
  set primary <dns_ipv4>
  set secondary <dns_ip4>
  set source-ip <ipv4_addr>
  set vdom-dns {disable | enable}
end
```

| Variable | Description | Default |
|-----------------------------|---|---------|
| ip6-primary <dns_ipv6> | Enter the primary IPv6 DNS server IP address. | :: |
| ip6-secondary <dns_ip6> | Enter the secondary IPv6 DNS server IP address. | :: |
| primary <dns_ipv4> | Enter the primary DNS server IP address. | 0.0.0.0 |
| secondary <dns_ip4> | Enter the secondary DNS IP server address. | 0.0.0.0 |
| source-ip <ipv4_addr> | Enter the source IP for communications to DNS server. | 0.0.0.0 |
| vdom-dns {disable enable} | Enable configuring DNS servers for the current VDOM. | disable |

vdom-link

Use this command to create an internal point-to-point interface object. This object is a link used to join virtual domains. Inter-VDOM links support BGP routing, and DHCP.

Creating the interface object also creates 2 new interface objects by the name of <name>0 and <name>1. For example if your object was named `v_link`, the 2 interface objects would be named `v_link0` and `v_link1`. You can then configure these new interfaces as you would any other virtual interface using `config system interface`.

When using vdom-links in HA, you can only have vdom-links in one vcluster. If you have vclusters defined, you must use the `vcluster` field to determine which vcluster will be allowed to contain the vdom-links.

A packet can pass through an inter-VDOM link a maximum of three times. This is to prevent a loop. When traffic is encrypted or decrypted it changes the content of the packets and this resets the inter-VDOM counter. However using IPsec or GRE tunnels do not reset the counter.

Syntax

```
config system vdom-link
  edit <name>
    set type {ppp | ethernet}
    set vcluster {1|2}
  end
```

| Variable | Description | Default |
|-----------------------|---|-------------|
| edit <name> | Enter the name of the link object to create. You are limited to 8 characters maximum for the name. | No default. |
| type {ppp ethernet} | Select type of VDOM link: PPP or Ethernet. | ppp |
| vcluster {1 2} | Select vcluster 1 or 2 as the only vcluster to have inter-VDOM links. This option is available only when HA and vclusters are configured, and there are VDOMs in both vclusters. | |

vdom-property

Use this command to enter a description of a VDOM and to configure resource usage for the VDOM that overrides global limits and specifies guaranteed resource usage for the VDOM.

When configuring resource usage for a VDOM you can set the *Maximum* and *Guaranteed* value for each resource.

- The Maximum value limits the amount of the resource that can be used by the VDOM. When you add a VDOM, all maximum resource usage settings are 0 indicating that resource limits for this VDOM are controlled by the global resource limits. You do not have to override the maximum settings unless you need to override global limits to further limit the resources available for the VDOM. You cannot set maximum resource usage higher in a VDOM than the corresponding global resource limit. For each resource you can override the global limit to reduce the amount of each resource available for this VDOM. The maximum must be the same as or lower than the global limit. The default value is 0, which means the maximum is the same as the global limit.



Use the command [“system resource-limits” on page 660](#) to set global resource limits.

- The Guaranteed value represents the minimum amount of the resource available for that VDOM. Setting the guaranteed value makes sure that other VDOMs do not use all of a resource. A guaranteed value of 0 means that an amount of this resource is not guaranteed for this VDOM. You only have to change guaranteed settings if your FortiGate may become low on resources and you want to guarantee that a minimum level is available for this VDOM. For each resource you can enter the minimum amount of the resource available to this VDOM regardless of usage by other VDOMs. The default value is 0, which means that an amount of this resource is not guaranteed for this VDOM.

Syntax

```
config global
  config system vdom-property
    edit <vdom_name>
      set custom-service <max_int> [<guaranteed_int>]
      set description <description_str>
      set dialup-tunnel <max_int> [<guaranteed_int>]
      set firewall-policy <max_int> [<guaranteed_int>]
      set firewall-profile <max_int> [<guaranteed_int>]
      set firewall-address <max_int> [<guaranteed_int>]
      set firewall-addrgrp <max_int> [<guaranteed_int>]
      set ipsec-phase1 <max_int> [<guaranteed_int>]
      set ipsec-phase2 <max_int> [<guaranteed_int>]
      set log-disk-quota <max_int>
      set onetime-schedule <max_int> [<guaranteed_int>]
      set recurring-schedule <max_int> [<guaranteed_int>]
      set service-group <max_int> [<guaranteed_int>]
      set session <max_int> [<guaranteed_int>]
      set user <max_int> [<guaranteed_int>]
      set user-group <max_int> [<guaranteed_int>]
```

```

    set web-proxy <max_int>
  end
end

```

| Variable | Description | Default |
|---|--|---------|
| edit <vdom_name> | Select the VDOM to set the limits for. | |
| custom-service <max_int> [<guaranteed_int>] | Enter the maximum and guaranteed number of firewall custom services. | 0 0 |
| description <description_str> | Enter a description of the VDOM. The description can be up to 63 characters long. | |
| dialup-tunnel <max_int> [<guaranteed_int>] | Enter the maximum and guaranteed number of dialup-tunnels. | 0 0 |
| firewall-policy <max_int> [<guaranteed_int>] | Enter the maximum and guaranteed number of firewall policies. | 0 0 |
| firewall-profile <max_int> [<guaranteed_int>] | Enter the maximum and guaranteed number of firewall profiles. | 0 0 |
| firewall-address <max_int> [<guaranteed_int>] | Enter the maximum and guaranteed number of firewall addresses. | 0 0 |
| firewall-addrgrp <max_int> [<guaranteed_int>] | Enter the maximum and guaranteed number of firewall address groups. | 0 0 |
| ipsec-phase1 <max_int> [<guaranteed_int>] | Enter the maximum and guaranteed number of IPSec phase1 tunnels. | 0 0 |
| ipsec-phase2 <max_int> [<guaranteed_int>] | Enter the maximum and guaranteed number of IPSec phase2 tunnels. | 0 0 |
| log-disk-quota <max_int> | Enter the maximum amount of log disk space available in MBytes for log messages for this VDOM. The range depends on the amount of hard disk space available. | 0 0 |
| onetime-schedule <max_int> [<guaranteed_int>] | Enter the maximum and guaranteed number of onetime schedules. | 0 0 |
| recurring-schedule <max_int> [<guaranteed_int>] | Enter the maximum and guaranteed number of recurring schedules. | 0 0 |
| service-group <max_int> [<guaranteed_int>] | Enter the maximum and guaranteed number of firewall service groups. | 0 0 |
| session <max_int> [<guaranteed_int>] | Enter the maximum and guaranteed number of sessions. | 0 0 |
| user <max_int> [<guaranteed_int>] | Enter the maximum and guaranteed number of users. | 0 0 |

| Variable | Description | Default |
|---|--|---------|
| user-group <max_int> [<guaranteed_int>] | Enter the maximum and guaranteed number of user groups. | 0 0 |
| web-proxy <max_int> | <p>Enter the maximum number of users that can be using the explicit web proxy at one time from this VDOM.</p> <p>How the number of concurrent explicit proxy users is determined depends on their authentication method:</p> <ul style="list-style-type: none">• For session-based authenticated users, each authenticated user is counted as a single user. Since multiple users can have the same user name, the proxy attempts to identify users according to their authentication membership (based upon whether they were authenticated using RADIUS, LDAP, FSSO, local database etc.). If a user of one session has the same name and membership as a user of another session, the explicit proxy assumes this is one user.• For IP Based authentication, or no authentication, or if no web-proxy firewall policy has been added, the source IP address is used to determine a user. All sessions from a single source address are assumed to be from the same user. | 0 0 |

vdom-radius-server

Use this command to specify the dynamic profile RADIUS server for each VDOM. This command is available only if VDOMs are enabled (vdom-admin is enabled in config system global).

Syntax

```
config system vdom-radius-server
edit vdom_name <name_str>
    set status {enable | disable}
    set radius-server-vdom <vdom_name_str>
end
```

| Variable | Description | Default |
|---------------------------------------|---|-------------|
| vdom_name <name_str> | Enter the VDOM name. | No default. |
| status {enable disable} | Enable or disable this VDOM RADIUS server entry. | disable |
| radius-server-vdom <vdom_name_str> | Enter the VDOM of the dynamic profile radius server to use for dynamic profile traffic in the current vdom. | No default. |

vdom-sflow

Use this command to add or change the IP address and UDP port that FortiGate sFlow agents operating on interfaces in a non-management VDOM use to send sFlow datagrams to an sFlow collector.

Syntax

```
config system sit-tunnel
  set collector-ip <collector_ipv4>
  set collector-port <collector_port_int>
  set vdom-sflow {enable | disable}
end
```

| Variable | Description | Default |
|----------------------------------|--|---------|
| collector-ip <collector_ipv4> | The IP address of the sFlow collector that sFlow agents added to interfaces in this VDOM should send sFlow datagrams to. | 0.0.0.0 |
| collector_port <port_int> | The UDP port number used for sending sFlow datagrams. Change this setting only if required by your sFlow collector or you network configuration. | 6343 |
| vdom-sflow {enable disable} | Enable configuring sFlow settings for the current VDOM. | enable |

virtual-switch

Use this command to configure virtual switch interfaces on the FortiGate models that support this feature.

Syntax

```
config system virtual-switch
  edit <vswitch_name>
    set physical-switch <switch_name>
    config port
      edit <port_name>
        set duplex {full | half}
        set speed <interface_speed>
        set status {up | down}
      end
    end
  end
```

| Variable | Description | Default |
|-----------------------------------|---|-------------|
| <vswitch_name> | Enter a name for the virtual switch. | No default. |
| set physical-switch <switch_name> | Enter the hardware switch name, sw0 for example. | |
| config port | Create an entry for each member interface. | |
| <port_name> | Enter the interface name. | |
| duplex {full half} | Select duplex setting. | full |
| speed <interface_speed> | Set the interface speed: auto — the default speed. The interface uses auto-negotiation to determine the connection speed. Change the speed only if the interface is connected to a device that does not support auto-negotiation. 10full — 10 Mbps, full duplex 10half — 10 Mbps, half duplex 100full — 100 Mbps, full duplex 100half — 100 Mbps, half duplex 1000full — 1000 Mbps, full duplex 1000half — 1000 Mbps, half duplex Speed options vary for different models and interfaces. Enter and a <code>set speed ?</code> to display a list of speeds available for your model and interface. | auto |
| status {up down} | Select up or down status for this member interface. | up |

wccp

Configure settings for Web Cache Communication Protocol (WCCP).

You can configure a FortiGate unit to operate as a WCCP router or client.

- A FortiGate unit operating as a WCCP router can intercept HTTP and HTTPS sessions and forward them to a web caching engine that caches web pages and returns cached content to the web browser.
- A FortiGate unit operating as a WCCP client can accept and forward WCCP sessions and use firewall policies to apply NAT, UTM, and other FortiGate security features to them. A FortiGate unit operates as a WCCP client only in NAT/Route mode (and not in Transparent mode)

Enter the following command to configure a FortiGate unit to operate as a WCCP router (this is the default FortiGate WCCP configuration):

```
config system settings
    set wccp-cache-engine disable
end
```

Enter the following command to configure a FortiGate unit to operate as a WCCP client:

```
config system settings
    set wccp-cache-engine enable
end
```

When you enter this command an interface named `w.<vdom_name>` is added to the FortiGate configuration (for example `w.root`). All WCCP sessions received by a FortiGate unit operating as a WCCP client are considered to be received at this interface and you can enter firewall policies for the WCCP traffic.

Syntax (WCCP router mode)

```
config system wccp
    edit <service-id>
        set router-id <interface_ipv4>
        set group-address <multicast_ipv4>
        set server-list <router1_ipv4> [<router2_ipv4> ...
            <router4_ipv4>]
        set authentication {disable | enable}
        set forward-method {GRE | L2 | any}
        set return-method {GRE | L2 | any}
        set assignment-method {HASH | MASK | any}
        set password <password_str>
    next
end
```


Syntax (WCCP client mode)

```

config system wccp
  edit <service-id>
    set cache-id <cache_engine_ip4>
    set group-address <multicast_ipv4>
    set router-list <server_ipv4mask>
    set authentication {disable | enable}
    set service-type {auto | dynamic | standard}
    set assignment-weight <weight_int>
    set assignment-bucket-format {cisco-implementation | wccp-v2}
    set password <password_str>
  next
end

```

| Variable | Description | Default |
|---|--|-----------------|
| <service-id> | Valid ID range is from 0 to 255. 0 for HTTP. | 1 |
| router-id <interface_ipv4> | An IP address known to all cache engines. This IP address identifies a FortiGate interface IP address to the cache engines. If all cache engines connect to the same FortiGate interface, then <interface_ipv4> can be 0.0.0.0, and the FortiGate unit uses the IP address of that interface as the router-id. If the cache engines can connect to different FortiGate interfaces, you must set router-id to a single IP address, and this IP address must be added to the configuration of the cache engines that connect to that interface. | 0.0.0.0 |
| cache-id <cache_engine_ip4> | The IP address of the cache engine if its IP address is not the same as the IP address of a FortiGate interface. If the IP address of the cache engine is the same as the IP address of the FortiGate interface on which you have enabled WCCP, the cache-id should be 0.0.0.0. | 0.0.0.0 |
| group-address <multicast_ipv4> | The IP multicast address used by the cache routers. 0.0.0.0 means the FortiGate unit ignores multicast WCCP traffic. Otherwise, group-address must be from 224.0.0.0 to 239.255.255.255. | 0.0.0.0 |
| server-list <router1_ipv4> [<router2_ipv4> ... <router4_ipv4>] | The IP address and net mask of up to four WCCP routers. | 0.0.0.0 0.0.0.0 |
| router-list <server_ipv4mask> | IP addresses of one or more WCCP routers that can communicate with a FortiGate unit operating as a WCCP cache engine. Separate multiple addresses with a space. | |
| authentication {disable enable} | Enable or disable using use MD5 authentication for the WCCP configuration. | disable |
| service-type {auto dynamic standard} | Set the WCCP service type used by the cache server. | auto |
| forward-method {GRE L2 any} | Specifies how the FortiGate unit forwards traffic to cache servers. If forward-method is any the cache server determines the forward method. | GRE |

| Variable | Description | Default |
|---|--|----------------------|
| return-method { GRE L2 any } | Specifies how a cache server declines a redirected packet and returns it to the FortiGate unit. If <code>return-method</code> is <code>any</code> the cache server determines the return method. | GRE |
| assignment-method { HASH MASK any } | Specifies which assignment method the FortiGate unit prefers. If <code>assignment-method</code> is <code>any</code> the cache server determines the assignment method. | HASH |
| assignment-weight <weight_int> | Set the assignment weight for the WCCP cache engine. The range is 0 to 255. | 0 |
| assignment-bucket-format { cisco-implementation wccp-v2 } | Set the assignment bucket format for the WCCP cache engine. | cisco-implementation |
| password <password_str> | The authentication password. Maximum length is 8 characters. | No default. |

zone

Use this command to add or edit zones.

In NAT/Route mode, you can group related interfaces or VLAN subinterfaces into zones. Grouping interfaces and subinterfaces into zones simplifies policy creation. For example, if you have two interfaces connected to the Internet, you can add both of these interfaces to the same zone. Then you can configure policies for connections to and from this zone, rather than to and from each interface.

In Transparent mode you can group related VLAN subinterfaces into zones and add these zones to virtual domains.

Syntax

```
config system zone
  edit <zone_name>
    set interface <name_str>
    set intrazone {allow | deny}
  end
```

| Variable | Description | Default |
|--------------------------|---|-------------|
| edit <zone_name> | Enter the name of a new or existing zone. | |
| interface <name_str> | Add the specified interface to this zone. You cannot add an interface if it belongs to another zone or if firewall policies are defined for it. | No default. |
| intrazone {allow deny} | Allow or deny traffic routing between different interfaces in the same zone. | deny |

user

This chapter covers:

- configuration of the FortiGate unit to use external authentication servers, including Windows Active Directory or other Directory Service servers
- configuration of user accounts and user groups for firewall policy authentication, administrator authentication and some types of VPN authentication
- configuration of peers and peer groups for IPSec VPN authentication and PKI user authentication

This chapter contains the following sections:

| | |
|--------------------------------------|--------------------------|
| Configuring users for authentication | local password-policy |
| ban | peer |
| device | peergrp |
| device-access-list | radius |
| device-category | setting |
| device-group | tacacs+ |
| fortitoken | |
| fsso | |
| fsso-polling | |
| group | |
| ldap | |

Configuring users for authentication

This chapter covers two types of user configuration:

- users authenticated by password
- users, sites or computers (peers) authenticated by certificate

Configuring users for password authentication

You need to set up authentication in the following order:

1. If external authentication is needed, configure the required servers.

- See [“user radius” on page 735](#).
- See [“user ldap” on page 726](#).
- See [“user tacacs+” on page 742](#)
- For Directory Service, see [“user fsso” on page 718](#).

2. Configure local user identities.

For each user, you can choose whether the FortiGate unit or an external authentication server verifies the password.

- See [“user local” on page 729](#).

3. Create user groups.

Add local users to each user group as appropriate. You can also add an authentication server to a user group. In this case, all users in the server’s database can authenticate to the FortiGate unit.

- See [“user group” on page 722](#).
- For Directory Service, also see [“user ban” on page 710](#).

Configuring peers for certificate authentication

If your FortiGate unit will host IPSec VPNs that authenticate clients using certificates, you need to prepare for certificate authentication as follows:

1. Import the CA certificates for clients who authenticate with a FortiGate unit VPN using certificates.

- See [“vpn certificate ca” on page 757](#).

2. Enter the certificate information for each VPN client (peer).

- See [“user peer” on page 732](#).

3. Create peer groups, if you have VPNs that authenticate by peer group. Assign the appropriate peers to each peer group.

- See [“user peergrp” on page 734](#).

ban

The FortiGate unit compiles a list of all users, IP addresses, or interfaces that have a quarantine/ban rule applied to them. The Banned User list in the FortiGate web-based interface shows all IP addresses and interfaces blocked by NAC (Network Access Control) quarantine, and all IP addresses, authenticated users, senders and interfaces blocked by DLP (Data Leak Prevention). All users or IP addresses on the Banned User list are blocked until they are removed from the list, and all sessions to an interface on the list are blocked until the interface is removed from the list. Each banned user configuration can have an expiry time/date to automatically remove it from the Banned User list, or the user must be removed from the list manually by the system administrator.



You cannot configure items in the Banned user list with the CLI, you must use the web-based manager. In the CLI, you can display the list items in the Banned User list using `get user ban`, and remove items from the list using the following command:

```
config user ban
    delete banid <ban_int>
end
```

Syntax (view only, cannot be configured)

```
config user ban
    edit banid <ban_int>
        set source {dlp-rule | dlp-compound | IPS | AV | DoS}
        set type {quarantine-src-ip | quarantine-dst-ip
            | quarantine-src-dst-ip | quarantine-intf | dlp-user
            | dlp-ip | dlp-sender | dlp-im}
        set cause {IPS (Intrusion Protection Sensor) | Antivirus (AV)
            | Data Leak Prevention (DLP)}
        set src-ip-addr <src_ip_addr>
        set protocol {smtp | pop3 | imap | http-post | http-get | ftp-
            put | ftp-get | nntp | aim | icq | msn | ym | smtps | pop3s
            | imaps | https-post | https_get}
        set dst-ip-addr <dst_ip_addr>
        set interface <interface_name>
        set ip-addr <ip_addr>
        set user <user_name>
        set sender <sender_name>
        set im-type {aim | icq | msn | yahoo}
        set im-name <im_name>
        set expires <ban_expiry_date>
        set created <system_date>
    end
end
```

| Variable | Description | Default |
|-----------------|--|-------------|
| banid <ban_int> | Enter the unique ID number of the banned user configuration. | No default. |

| Variable | Description | Default |
|---|--|-------------------|
| source {dlp-rule dlp-compound IPS AV DoS} | The source of the ban: <ul style="list-style-type: none"> dlp-rule – a DLP rule configured by the system administrator dlp-compound – a DLP compound rule configured by the system administrator IPS – FortiGate unit IPS AV – FortiGate unit IPS DoS – DoS sensor | dlp-rule |
| type {quarantine-src-ip quarantine-dst-ip quarantine-src-dst-ip quarantine-intf dlp-user dlp-ip dlp-sender dlp-im} | The type of ban: <ul style="list-style-type: none"> quarantine-src-ip – Complete quarantine based on source IP address quarantine-dst-ip – Complete quarantine based on destination IP address quarantine-src-dst-ip – Block all traffic from source to destination address quarantine-intf – Block all traffic on the banned interface (port quarantine) dlp-user – Ban based on user dlp-ip – Ban based on IP address of user dlp-sender – Ban based on email sender dlp-im – Ban based on IM user | quarantine-src-ip |
| cause {IPS (Intrusion Protection Sensor) Antivirus (AV) Data Leak Prevention (DLP)} | FortiGate function that caused ban: <ul style="list-style-type: none"> IPS (Intrusion Protection Sensor) Antivirus (AV) – virus detected Data Leak Prevention (DLP) | (null) |
| src-ip-addr <src_ip_addr> | The banned source IP address. | 0.0.0.0 |
| protocol {smtp pop3 imap http-post http-get ftp-put ftp-get nntp aim icq msn ym smtps pop3s imaps https-post https_get} | The protocol used by the user or IP addresses added to the Banned User list. | No default. |
| dst-ip-addr <dst_ip_addr> | The destination IP address quarantined or banned. This applies to ban types quarantine-dst-ip and quarantine-src-dst-ip. | |
| interface <interface_name> | The interface that was quarantined or banned. This applies to ban type quarantine-intf. | null |
| ip-addr <ip_addr> | The banned IP address (ban type dlp-ip). | 0.0.0.0 |
| user <user_name> | The name of the banned user (ban type dlp-user). | null |
| sender <sender_name> | The name of the banned sender (ban type dlp-sender). | null |

| Variable | Description | Default |
|-------------------------------------|--|-------------|
| im-type { aim icq msn yahoo } | The type of instant messenger that was banned. This applies to ban type <code>dlp-im</code> : <ul style="list-style-type: none">aim – AOL instant messengericq – ICQmsn – MSN messengeryahoo – Yahoo! messenger | aim |
| im-name <im_name> | The name of the banned instant messenger (ban type <code>dlp-im</code>). | null |
| expires <ban_expiry_date> | Date and Time when the FortiGate unit will lift the ban. Date and time <yyyy/mm/dd hh:mm:ss>. Range from 5 minutes to 365 days or indefinite. If set to <code>indefinite</code> , the ban must be manually removed from the Banned User list. | indefinite |
| created <system_date> | System-generated time that the ban was created by the system administrator. Format <code>Wed Dec 31 16:00:00 1969</code> . | No default. |

device

Use this command to define host devices.

Syntax

```
config user device
  edit <device_alias>
    set comment <comment_str>
    set mac <mac_addr>
    set type {android-phone | android-tablet | blackberry-phone |
             blackberry-playbook | fortinet-device | gaming-console |
             ip-phone | linux-pc | mac | media-streaming | other-
             network-device | windows-pc | windows-phone | ipad | iphone
             | router-nat-device}
    set user <username_str>
  end
```

| Variable | Description | Default |
|---|---|-------------------|
| <device_alias> | Enter a name for the device. Device, device type and device group names must be unique. | No default. |
| comment <comment_str> | Optionally, enter a comment up to 32 characters in length. | No default. |
| mac <mac_addr> | Enter the MAC address of the device. | 00:00:00:00:00:00 |
| type {android-phone android-tablet blackberry-phone blackberry-playbook fortinet-device gaming-console ip-phone linux-pc mac media-streaming other-network-device windows-pc windows-phone ipad iphone router-nat-device} | Select the device type. | Null |
| user <username_str> | Enter the name of the device's user. | Null |

device-access-list

Use this command to configure device lists for use on interfaces with device identification enabled.

Syntax

```
config user device-access-list
  edit <devlist_name>
    set default-action {accept | deny}
    config device-list
      edit <id>
        set action {accept | deny}
        set device <dev_name>
      end
    end
  end
```

| Variable | Description | Default |
|--------------------------------|--|-------------|
| <devlist_name> | Enter a name for this device list. | |
| action {accept deny} | Select whether to accept or deny this device. | |
| default-action {accept deny} | Select whether to allow or deny unknown devices. | accept |
| device <dev_name> | Enter the device name. | No default. |

device-category

Use this command to provide comments for the predefined device types. You cannot create or delete device types.

Syntax

```
config user device-category
  edit {android-phone | android-tablet | blackberry-phone
      | blackberry-playbook | collected-emails | fortinet-device
      | gaming-console | ip-phone | ipad | iphone | linux-pc | mac
      | media-streaming | other-network-device | router-nat-device
      | windows-pc | windows-phone}
    set comment <comment_str>
  end
```

| Variable | Description | Default |
|-----------------------|--------------------------|-------------|
| comment <comment_str> | Comment (read-only). | No default. |
| desc <desc_str> | Description (read-only). | No default. |

device-group

Use this command to define device groups.

Syntax

```
config user device-group
  edit <groupname_str>
    set comment <comment_str>
    set member {device-1 ... device-n}
  end
```

| Variable | Description | Default |
|--------------------------------|--|-------------|
| <groupname_str> | Enter a name for this device group. Device, device type and device group names must be unique. | No default. |
| comment <comment_str> | Optionally, enter a comment up to 32 characters in length. | No default. |
| member {device-1 ... device-n} | Enter the device names that belong to this group. | No default. |

fortitoken

This command to register FortiToken devices and FortiToken Mobile “soft token” certificates.

Syntax

```
config user fortitoken
  edit serial-number <sn_str>
    set status {active | lock}
    set comments <comment_str>
    set license <license_str>
    set activation-code <code_str>
    set activation-expire <str>
  end
```

| Variable | Description | Default |
|----------------------------|--|-------------|
| serial-number <sn_str> | Enter the FortiToken device serial number. | No default. |
| status {active lock} | Activate or lock out FortiToken device. | active |
| comments <comment_str> | | No default. |
| license <license_str> | FortiToken Mobile license. You can retrieve this using the command <code>execute fortitoken-mobile import <activation_code></code> | No default. |
| activation-code <code_str> | Displays the FortiToken activation code from the FortiToken Mobile account. You cannot change this setting. | No default. |
| activation-expire <str> | Displays the activation expiry time as set by the <code>config system global option two-factor-ftm-expiry</code> . | No default |

fssso

Use this command to configure the FortiGate unit to receive user group information from a Directory Service server equipped with the Fortinet Single Sign On Agent (FSSO-Agent). You can specify up to five computers on which a FSSO collector agent is installed. The FortiGate unit uses these collector agents in a redundant configuration. If the first agent fails, the FortiGate unit attempts to connect to the next agent in the list.

You can add user groups to Directory Service type user groups for authentication in firewall policies.

Syntax

```
config user fssso
  edit <server_name>
    set ldap_server <ldap-server-name>
    set password <password>
    set password2 <password2>
    set password3 <password3>
    set password4 <password4>
    set password5 <password5>
    set port <port_number>
    set port2 <port2_number>
    set port3 <port3_number>
    set port4 <port4_number>
    set port5 <port5_number>
    set server <domain>
    set server2 <domain2>
    set server3 <domain3>
    set server4 <domain4>
    set server5 <domain5>
    set source-ip <ipv4_addr>
  end
```

| Variable | Description | Default |
|---|---|-------------|
| edit <server_name> | Enter a name to identify the Directory Service server. Enter a new name to create a new server definition or enter an existing server name to edit that server definition. | No default. |
| ldap_server <ldap-server-name> | Enter the name of the LDAP server to be used to access the Directory Service. | No default. |
| password <password> password2 <password2> password3 <password3> password4 <password4> password5 <password5> | For each collector agent, enter the password. | No default. |

| Variable | Description | Default |
|--|---|-------------|
| port <port_number> port2 <port2_number> port3 <port3_number> port4 <port4_number> port5 <port5_number> | For each collector agent, enter the port number used for communication with FortiGate units. | 8000 |
| server <domain> server2 <domain2> server3 <domain3> server4 <domain4> server5 <domain5> | Enter the domain name or IP address for up to five collector agents. Range from 1 to 63 characters. | No default. |
| source-ip <ipv4_addr> | Enter the source IP for communications to FSSO server. | 0.0.0.0 |

fsso-polling

Use this command to configure polling of servers for Fortinet Single Sign-On.

Syntax - Global

```
config user fsso-polling
  edit <AD_id_int>
    set status {enable | disable}
    set server <name>
    set authentication {enable | disable}
    set auth-password <pwd_str>
    set listening-port <port_int>
  end
```

Syntax - VDOM

```
config user fsso-polling
  edit <AD_id_int>
    set status {enable | disable}
    set server <name>
    set password <pwd_str>
    set default-domain <domain_str>
    set ldap-server <server_name>
    set logon-history <hours_int>
    set polling-frequency <sec_int>
    set port <port_int>
    set user <uid_str>
  config adgrp
    edit adgrp-name <group_name>
  end
end
```

| Variable | Description | Default |
|-----------------------------------|--|---------|
| <AD_id_int> | Enter an ID number for the Windows Active Directory (AD) server. | |
| status {enable disable} | Enable or disable FSSO polling. | enable |
| server <name> | Enter the AD server name or IP address. | Null |
| password <pwd_str> | Enter the AD server password. | Null |
| authentication {enable disable} | Enable or disable authentication. | enable |
| auth-password <pwd_str> | Enter the AD server password. | Null |
| default-domain <domain_str> | Enter this server's default domain name. | Null |
| ldap-server <server_name> | Enter the name of the LDAP server for group and user names. | Null |
| listening-port <port_int> | Enter the server port number. Range 1 to 65535. | 8000 |
| logon-history <hours_int> | Enter length of logon history. Range 1 to 48 hours. | 8 |
| polling-frequency <sec_int> | Enter the polling interval. Range 1 to 30 seconds. | 10 |

| Variable | Description | Default |
|----------------------------|---|-------------|
| port <port_int> | Enter the server port number. Range 0 the 65 535. | 0 |
| user <uid_str> | Enter the user account name for the AD server. | Null |
| config adgrp fields | | |
| adgrp-name <group_name> | Enter a Windows AD group name for which FSSO polling will be conducted. | No default. |

group

Use this command to add or edit user groups. User groups can include defined peer members.

Syntax

```
config user group
  edit <groupname>
    set auth-concurrent-override {enable | disable}
    set auth-concurrent-value <limit_int>
    set authtimeout <timeout>
    set company {disabled | mandatory | optional}
    set email {enable | disable}
    set expire <seconds_int>
    set expire-type {immediately | first-successful-login}
    set group-type {firewall | fsso-service | rsoo | guest}
    set http-digest-realm <realm_str>
    set member <names>
    set mobile-phone {enable | disable}
    set multiple-guest-add {enable | disable}
    set password {auto-generate | email | specify}
    set sponsor {disabled | mandatory | optional}
    set sslvpn-portal <web_portal_name>
    set sso-attribute-value <string>
    set user-id {auto-generate | email | specify}
    set user-name {enable | disable}
  config guest
    edit <guest_id>
      set company <company-name_str>
      set email <email-addr_str>
      set expiration <expire-time_str>
      set mobile-phone <telnumber_str>
      set name <name_str>
      set password <pwd_str>
      set sponser <sponsor-name_str>
    end
  config match
    edit <match_id>
      set group-name <gname_str>
      set rsoo {enable | disable}
      set server-name <srvname_str>
    end
  end
end
```

| Variable | Description | Default |
|---|--|-------------|
| edit <groupname> | Enter a new name to create a new group or enter an existing group name to edit that group. | No default. |
| auth-concurrent-override {enable disable} | Enable to override the policy-auth-concurrent setting in system global . | disable |

| Variable | Description | Default |
|--|---|-------------|
| auth-concurrent-value <limit_int> | Set the number of concurrent logins permitted from the same user. Range 1 to 100. 0 means no limit. This field is available if auth-concurrent-override is enabled. | 0 |
| authtimeout <timeout> | Enter the value in seconds of an authentication timeout for the user group. Range 1 to 480 minutes. Enter 0 to use the global authentication value. This is available if group-type is firewall or directory-service. | 0 |
| company {disabled mandatory optional} | Select the option for the guest's company name field on the web-based manager Guest Management form: disabled, mandatory or optional. This is available if group-type is guest. | optional |
| email {enable disable} | Enable or disable the email address field in the web-based manager Guest Management form. This is available if group-type is guest. | disable |
| expire <seconds_int> | Enter the number of seconds until the guest account expires. This is available if group-type is guest. | 14400 |
| expire-type {immediately first-successful-login} | Select when expiry time countdown begins: immediately or after the user's first successful login. This is available if group-type is guest. | immediately |
| group-type {firewall fsso-service rso guest} | Enter the group type. <grp_type> determines the type of user: firewall - FortiGate users defined in user local, user ldap or user radius fsso-service - Single Sign On users rso - RADIUS SSO users guest - guest users | firewall |
| http-digest-realm <realm_str> | Enter the realm attribute for MD5-digest authentication. | No default. |
| member <names> | Enter the names of users, peers, LDAP servers, or RADIUS servers to add to the user group. Separate names by spaces. To add or remove names from the group you must re-enter the whole list with the additions or deletions required. This field is available if group-type is firewall or fsso-service. | No default. |
| mobile-phone {enable disable} | Enable or disable the mobile phone number field in the web-based manager Guest Management form. This is available if group-type is guest. | disable |
| multiple-guest-add {enable disable} | Enable or disable the multiple guest add option in the web-based manager User Group form. This is available if group-type is guest. | disable |

| Variable | Description | Default |
|---|---|---------------|
| password { auto-generate email specify } | Select the source of the guest password: auto-generate — create a random user ID email — use the guest's email address specify — enter a user ID string This is available if group-type is guest. | auto-generate |
| sponsor { disabled mandatory optional } | Select whether the sponsor field on the web-based manager Guest Management form should be disabled, mandatory or optional. This is available if group-type is guest. | optional |
| sslvpn-portal <web_portal_name> | Enter the name of the SSL-VPN portal for this group. This is available if group-type is sslvpn. | No default. |
| sso-attribute-value <string> | Enter the name of the RADIUS user group this local user group represents. | No default. |
| user-id { auto-generate email specify } | Select the source of the guest user ID: auto-generate — create a random user ID email — use the guest's email address specify — enter a user ID string This is available if group-type is guest. | email |
| user-name { enable disable } | Enable or disable guest user name entry. This is available if group-type is guest. | disable |
| config guest fields | Configure guest users. This is available if group-type is guest. | |
| <guest_id> | Enter the guest user ID. | No default. |
| company <company-name_str> | Enter the user's company name. | |
| email <email-addr_str> | Enter the user's email address. | |
| expiration <expire-time_str> | Enter the account expiration time. | |
| mobile-phone <telnumber_str> | Enter the user's user's telephone number. | |
| name <name_str> | Enter the user's name. | |
| password <pwd_str> | Enter the user's password. | |
| ponser <sponsor-name_str> | Enter the user's sponsor. | |
| config match fields | Specify the user group names on the authentication servers that are members of this FortiGate user group. If no matches are specified, all users on the server can authenticate. | |
| <match_id> | Enter an ID for the entry. | |
| group-name <gname_str> | The name of the matching group on the remote authentication server. | |

| Variable | Description | Default |
|---------------------------|--|---------|
| rsso {enable disable} | Enable or disable RADIUS single sign-on matching in this user group. | disable |
| server-name <srvname_str> | The name of the remote authentication server. | |

Ldap

Use this command to add or edit the definition of an LDAP server for user authentication.

To authenticate with the FortiGate unit, the user enters a user name and password. The FortiGate unit sends this user name and password to the LDAP server. If the LDAP server can authenticate the user, the user is successfully authenticated with the FortiGate unit. If the LDAP server cannot authenticate the user, the connection is refused by the FortiGate unit. The maximum number of remote LDAP servers that can be configured for authentication is 10.

The FortiGate unit supports LDAP protocol functionality defined in RFC2251 for looking up and validating user names and passwords. FortiGate LDAP supports all LDAP servers compliant with LDAP v3.

FortiGate LDAP support does not extend to proprietary functionality, such as notification of password expiration, that is available from some LDAP servers. FortiGate LDAP support does not supply information to the user about why authentication failed.

LDAP user authentication is supported for PPTP, L2TP, IPsec VPN, and firewall authentication. With PPTP, L2TP, and IPsec VPN, PAP (Packet Authentication Protocol) is supported and CHAP (Challenge Handshake Authentication Protocol) is not.

Syntax

```
config user ldap
    edit <server_name>
        set cnid <id>
        set dn <dnname>
        set group-member-check {user-attr | group-object}
        set group-object-filter <group_filter>
        set member-attr <attr_name>
        set port <number>
        set server <domain>
        set secondary-server <domain>
        set tertiary-server <domain>
        set source-ip <source_ipv4addr>
        set type <auth_type>
        set username <ldap_username>
        set password <ldap_passwd>
        set password-expiry-warning {disable | enable}
        set password-renewal {disable | enable}
        set secure <auth_port>
        set ca-cert <cert_name>
    end
```

| Variable | Description | Default |
|--------------------|--|-------------|
| edit <server_name> | Enter a name to identify the LDAP server. Enter a new name to create a new server definition or enter an existing server name to edit that server definition. | No default. |

| Variable | Description | Default |
|---|--|-------------|
| cnid <id> | Enter the common name identifier for the LDAP server. The common name identifier for most LDAP servers is cn. However some servers use other common name identifiers such as uid. Maximum 20 characters. | cn |
| dn <dnname> | Enter the distinguished name used to look up entries on the LDAP server. It reflects the hierarchy of LDAP database object classes above the Common Name Identifier. The FortiGate unit passes this distinguished name unchanged to the server. You must provide a dn value if type is simple. Maximum 512 characters. | No default. |
| group-member-check {user-attr group-object} | Select the group membership checking method: user attribute or group object. | user-attr |
| group-object-filter <group_filter> | Enter the name of the filter for group searches. The search for the group on the LDAP server is done with the following default filter configuration: (&(objectcategory=group) (member=*)) For example, to look for the group that will allow dial-in (msNPAllowDialin) set the filter to (&(uid=%u) (msNPAllowDialin=TRUE)). This field is available when group-member-check is group-object. | |
| member-attr <attr_name> | An attribute of the group that is used to authenticate users. | null |
| port <number> | Enter the port number for communication with the LDAP server. | 389 |
| server <domain> | Enter the LDAP server domain name or IP address. The host name must comply with RFC1035. | No default. |
| secondary-server <domain> | Optionally, enter a second LDAP server name or IP address. | No default. |
| tertiary-server <domain> | Optionally, enter a third LDAP server name or IP address. | No default. |
| source-ip <source_ip4addr> | Optionally, enter a source IP address to use for LDAP requests. | 0.0.0.0 |

| Variable | Description | Default |
|--|---|----------------------|
| type <auth_type> | <p>Enter the authentication type for LDAP searches. One of:</p> <ul style="list-style-type: none"> <code>anonymous</code> — bind using anonymous user search <code>regular</code> — bind using username/password and then search <code>simple</code> — simple password authentication without search <p>You can use <code>simple</code> authentication if the user records are all under one <code>dn</code> that you know. If the users are under more than one <code>dn</code>, use the <code>anonymous</code> or <code>regular</code> type, which can search the entire LDAP database for the required user name.</p> <p>If your LDAP server requires authentication to perform searches, use the <code>regular</code> type and provide values for <code>username</code> and <code>password</code>.</p> | <code>simple</code> |
| username <ldap_username> | This field is available only if <code>type</code> is <code>regular</code> . For <code>regular</code> authentication, you need a user name and password. See your server administrator for more information. | No default. |
| password <ldap_passwd> | This field is available only if <code>type</code> is <code>regular</code> . For <code>regular</code> authentication, you need a user name and password. See your server administrator for more information. | No default. |
| password-expiry-warning {disable enable} | Enable or disable password expiry warnings. | <code>disable</code> |
| password-renewal {disable enable} | Enable or disable online password renewal. | <code>disable</code> |
| secure <auth_port> {disable starttls ldaps} | <p>Select the port to be used in authentication.</p> <p><code>disable</code> — port 389</p> <p><code>ldaps</code> — port 636</p> <p><code>starttls</code> — port 389</p> | <code>disable</code> |
| ca-cert <cert_name> | This field is available when <code>secure</code> is set to <code>ldaps</code> or <code>starttls</code> . User authentication will take place via a CA certificate. The CA certificate will be used by the LDAP library to validate the public certificate provided by the LDAP server. | <code>null</code> |

local

Use this command to add local user names and configure user authentication for the FortiGate unit. To add authentication by LDAP or RADIUS server you must first add servers using the `config user ldap` and `config user radius` commands.

Syntax

```
config user local
  edit <username>
    set auth-concurrent-override {enable | disable}
    set auth-concurrent-value <limit_int>
    set ldap-server <servername>
    set passwd <password_str>
    set passwd-policy <policy_name>
    set passwd-time <time_str>
    set radius-server <servername>
    set sms-custom-server <srv_name>
    set sms-phone <phone_str>
    set sms-server {fortiguard | custom}
    set status {enable | disable}
    set tacacs+-server <servername>
    set two-factor {disable | fortitoken | email | sms}
    set type <auth-type>
    set workstation <name_str>
  end
```

| Variable | Description | Default |
|--|--|-------------|
| edit <username> | Enter the user name. Enter a new name to create a new user account or enter an existing user name to edit that account. | |
| auth-concurrent-override {enable disable} | Enable to override the policy-auth-concurrent setting in system global . | disable |
| auth-concurrent-value <limit_int> | Set the number of concurrent logins permitted from the same IP address. Range 1 to 100. 0 means no limit. This field is available if auth-concurrent-override is enabled. | 0 |
| ldap-server <servername> | Enter the name of the LDAP server with which the user must authenticate. You can only select an LDAP server that has been added to the list of LDAP servers. See “ldap” on page 726 . This is available when type is set to ldap. | No default. |
| passwd <password_str> | Enter the password with which the user must authenticate. Passwords at least 6 characters long provide better security than shorter passwords. This is available when type is set to password. | No default. |
| passwd-policy <policy_name> | Optionally, select a password policy to apply to this user. Use user password-policy to create password policies. | null |
| passwd-time <time_str> | The time of last password update. (Read only). | No default. |

| Variable | Description | Default |
|--|---|-------------|
| radius-server <servername> | Enter the name of the RADIUS server with which the user must authenticate. You can only select a RADIUS server that has been added to the list of RADIUS servers. See “radius” on page 735 . This is available when <code>type</code> is set to <code>radius</code> . | No default. |
| sms-custom-server <srv_name> | Enter the custom server to use for SMS-based two-factor authentication. The server name must be defined first using the <code>config system sms-server</code> command. This field is available when <code>two-factor</code> is <code>sms</code> and <code>sms-server</code> is <code>custom</code> . | No default. |
| sms-phone <phone_str> | Enter the user's phone number for SMS-based two-factor authentication. | No default. |
| sms-server {fortiguard custom} | Select FortiGuard or custom SMS server for SMS-based two-factor authentication. This field is available when <code>two-factor</code> is <code>sms</code> . | fortiguard |
| status {enable disable} | Enter <code>enable</code> to allow the local user to authenticate with the FortiGate unit. | enable |
| tacacs+-server <servername> | Enter the name of the TACACS+ server with which the user must authenticate. You can only select a TACACS+ server that has been added to the list of TACACS+ servers. See “tacacs+” on page 742 . This is available when <code>type</code> is set to <code>tacacs+</code> . | No default. |
| two-factor {disable fortitoken email sms} | Enable two-factor authentication through FortiToken, email, or SMS. | disable |
| type <auth-type> | Enter one of the following to specify how this user's password is verified: <code>ldap</code> — The LDAP server specified in <code>ldap-server</code> verifies the password. <code>password</code> — The FortiGate unit verifies the password against the value of <code>passwd</code> . <code>radius</code> — The RADIUS server specified in <code>radius-server</code> verifies the password. <code>tacacs+</code> — The TACACS+ server specified in <code>tacacs+-server</code> verifies the password. | No default. |
| workstation <name_str> | Enter the user's workstation name if you want to permit the user to authenticate only from a particular workstation. This is available when <code>type</code> is <code>ldap</code> . | null |

password-policy

Use this command to define password policies that set user password expiry and provide expiry warnings.

Syntax

```
config user password-policy
  edit <policy_name>
    set expire-days <days_int>
    set warn-days <days_int>
  end
```

| Variable | Description | Default |
|------------------------|--|-------------|
| <policy_name> | Enter a name for this password policy. | No default. |
| expire-days <days_int> | Set the number of days until expiry. Range 0 to 999. | 180 |
| warn-days <days_int> | Set number of days prior to expiry to provide expiry warning. Range 0 to 30. | 15 |

peer

Use this command to add or edit peer (digital certificate holder) information. You use the peers you define here in the `config vpn ipsec phase1` command if you specify `peertype` as `peer`. Also, you can add these peers to peer groups you define in the `config user peergrp` command.

For PKI user authentication, you can add or edit peer information and configure use of LDAP server to check access rights for client certificates.

This command refers to certificates imported into the FortiGate unit. You import CA certificates using the `vpn certificate ca` command. You import local certificates using the `vpn certificate local` command.

You can configure a peer user with no values in `subject` or `ca`. This user behaves like a user account or policy that is disabled.



If you create a PKI user in the CLI with no values in `subject` or `ca`, you cannot open the user record in the web-based manager, or you will be prompted to add a value in Subject (`subject`) or CA (`ca`).

Syntax

```
config user peer
  edit <peer_name>
    set ca <ca_name>
    set cn <cn_name>
    set cn-type <type>
    set ldap-mode {password | principal-name}
    set ldap-password <ldap_password>
    set ldap-server <ldap_server>
    set ldap-username <ldap_user>
    set mandatory-ca-verify {enable | disable}
    set ocsp-override-server <ocsp-name>
    set passwd <password_str>
    set subject <constraints>
    set two-factor {enable | disable}
  end
```

| Variable | Description | Default |
|------------------|--|-------------|
| edit <peer_name> | Enter the peer name. Enter a new name to create a new peer or enter an existing peer name to edit that peer's information. | |
| ca <ca_name> | Enter the CA certificate name, as returned by <code>execute vpn certificate ca list</code> . | No default. |
| cn <cn_name> | Enter the peer certificate common name. | No default. |

| Variable | Description | Default |
|---|--|-------------|
| cn-type <type> | Enter the peer certificate common name type: FQDN — Fully-qualified domain name. email — The user's email address. ipv4 — The user's IP address (IPv4). ipv6 — The user's IP address (IPv6). string — Any other piece of information. | string |
| ldap-mode {password principal-name} | Select mode for LDAP authentication. password — use user name and password. principal-name — use LDAP userPrincipalName attribute. | password |
| ldap-password <ldap_password> | Enter the login password for the LDAP server used to perform client access rights check for the defined peer. | No default. |
| ldap-server <ldap_server> | Enter the name of one of the LDAP servers defined under 'config user ldap' used to perform client access rights check for the defined peer. | null |
| ldap-username <ldap_user> | Enter the login name for the LDAP server used to perform client access rights check for the defined peer. | null |
| mandatory-ca-verify {enable disable} | If the CA certificate is installed on the FortiGate unit, the peer certificate is checked for validity. The mandatory-ca-verify field determines what to do if the CA certificate is not installed: enable — The peer cannot be authenticated. disable — The peer certificate is automatically considered valid and authentication succeeds. | disable |
| ocsp-override-server <ocsp-name> | Enter the OCSP server to use to retrieve certificate. This applies if OCSP is enabled in vpn certificate setting. | null |
| passwd <password_str> | Enter the password that this peer uses for two-factor authentication. The is available when two-factor is enabled. | No default. |
| subject <constraints> | Optionally, enter any of the peer certificate name constraints. | No default. |
| two-factor {enable disable} | Enable user to authenticate by password in addition to certificate authentication. Specify the password in passwd. | disable |

peergrp

Use this command to add or edit a peer group. Peers are digital certificate holders defined using the `config user peer` command. You use the peer groups you define here in the `config vpn ipsec phase1` command if you specify `peertype` as `peergrp`.

For PKI user authentication, you can add or edit peer group member information. User groups that use PKI authentication can also be configured using `config user group`.

Syntax

```
config user peergrp
  edit <groupname>
    set member <peer_names>
  end
```

| Variable | Description | Default |
|---------------------|---|-------------|
| edit <groupname> | Enter a new name to create a new peer group or enter an existing group name to edit that group. | |
| member <peer_names> | Enter the names of peers to add to the peer group. Separate names by spaces. To add or remove names from the group you must re-enter the whole list with the additions or deletions required. | No default. |

radius

Use this command to add or edit the information used for RADIUS authentication.

The default port for RADIUS traffic is 1812. If your RADIUS server is using a different port you can change the default RADIUS port. You may set a different port for each of your RADIUS servers. The maximum number of remote RADIUS servers that can be configured for authentication is 10.

The RADIUS server is now provided with more information to make authentication decisions, based on values in `server`, `use-management-vdom`, `nas-ip`, and the `config user group subcommand config match`. Attributes include:

- `NAS-IP-Address` - RADIUS setting or IP address of FortiGate interface used to talk to RADIUS server, if not configured
- `NAS-Port` - physical interface number of the traffic that triggered the authentication
- `Called-Station-ID` - same value as NAS-IP Address but in text format
- `Fortinet-Vdom-Name` - name of VDOM of the traffic that triggered the authentication
- `NAS-Identifier` - configured hostname in non-HA mode; HA cluster group name in HA mode
- `Acct-Session-ID` - unique ID identifying the authentication session
- `Connect-Info` - identifies the service for which the authentication is being performed (web-auth, vpn-ipsec, vpn-pptp, vpn-l2tp, vpn-ssl, admin-login, test)

You may select an alternative authentication method for each server. These include CHAP, PAP, MS-CHAP, and MS-CHAP-v2.

Syntax

```
config user radius
  edit <server_name>
    set all-usergroup {enable | disable}
    set auth-type {auto | chap | ms_chap | ms_chap_v2 | pap}
    set h3c-compatibility {enable | disable}
    set nas-ip <use_ip>
    set radius-port <radius_port_num>
    set secret <server_password>
    set server <domain>
    set secondary-secret <sec_server_password>
    set secondary-server <sec_server_domain>
    set tertiary-secret <ter_server_password>
    set tertiary-server <ter_domain>
    set source-ip <ipv4_addr>
    set use-management-vdom {enable | disable}
    set rso {enable | disable}
    set rso-context-timeout <timeout_seconds>
    set rso-endpoint-attribute <RADIUS_attribute>
    set rso-endpoint-block-attribute <RADIUS_attribute>
    set rso-flush-ip-session {enable | disable}
    set rso-log-flags <lflags>
    set rso-log-period <log_time>
    set rso-radius-response {enable | disable}
```

```

set rso-radius-server-port <RADIUS_listen_port>
set rso-secret <server_password>
set rso-validate-request-secret {enable | disable}
set sso-attribute <RADIUS_attribute>
set sso-attribute-key <profile_attribute_key>
config accounting-server
  edit <id_int>
    set status {enable | disable}
    set server <domain | IP>
    set secret <server_password>
    set source-ip <ipv4_addr>
  end
end

```

| Variable | Description | Default |
|--|---|-------------|
| edit <server_name> | Enter a name to identify the RADIUS server. Enter a new name to create a new server definition or enter an existing server name to edit that server definition. | |
| all-usergroup {enable disable} | Enable to automatically include this RADIUS server in all user groups. | disable |
| auth-type {auto chap ms_chap ms_chap_v2 pap} | Select the authentication method for this RADIUS server. auto uses pap, ms_chap_v2, and chap. | auto |
| h3c-compatibility {enable disable} | Enable compatibility with the H3C Intelligent Management Platform (IMC) server. The supplicant requests 802.1X authentication and then sends a second phase security check request to the H3C IMC server. | disable |
| nas-ip <use_ip> | IP address used as NAS-IP-Address and Called-Station-ID attribute in RADIUS access requests. RADIUS setting or IP address of FGT interface used to talk with RADIUS server, if not configured. | No default. |
| radius-port <radius_port_num> | Change the default RADIUS port for this server. The default port for RADIUS traffic is 1812. Range is 0..65535. | 1812 |
| secret <server_password> | Enter the RADIUS server shared secret. The server secret key should be a maximum of 16 characters in length. | No default. |
| server <domain> | Enter the RADIUS server domain name or IP address. The host name must comply with RFC1035. | No default. |
| secondary-secret <sec_server_password> | Enter the secondary RADIUS server shared secret. The server secret key should be a maximum of 16 characters in length. | No default. |
| secondary-server <sec_server_domain> | Enter the secondary RADIUS server domain name or IP address. | No default. |
| tertiary-secret <ter_server_password> | Enter the tertiary RADIUS server shared secret. The server secret key should be a maximum of 16 characters in length. | No default. |
| tertiary-server <ter_domain> | Optionally, enter the secondary RADIUS server domain name or IP address. | No default. |

| Variable | Description | Default |
|--|--|---------|
| source-ip <ipv4_addr> | Enter the source IP for communications to RADIUS server. | 0.0.0.0 |
| use-management-vdom {enable disable} | Enable to use the management VDOM to send all RADIUS requests. | disable |

| Variable | Description | Default |
|--|--|-------------|
| config accounting-server fields | | |
| status {enable disable} | Enable or disable accounting server configuration. | disable |
| server <domain IP> | Enter the accounting server domain name or IP address. | No default. |
| secret <server_password> | Enter the accounting server shared secret. The server secret key should be a maximum of 16 characters in length. | No default. |
| source-ip <ipv4_addr> | Enter the source IP for communications to the accounting server. | 0.0.0.0 |

| Variable | Description | Default |
|--|---|---------|
| RADIUS SSO fields | | |
| rsso {enable disable} | Enable RADIUS SSO to configure a RADIUS SSO agent. Then, FortiOS accepts connections on the <code>rsso-radius-server-port</code> . Other RSSO settings become available. | disable |
| rsso-context-timeout <timeout_seconds> | <p>When the FortiGate unit receives a RADIUS Start record, the user added to a “user context list” of logged on users. The user is considered logged on until</p> <ul style="list-style-type: none"> the FortiGate unit receives a RADIUS Stop record for the user’s end point <p>or</p> <ul style="list-style-type: none"> this timeout period has expired with no communication from the user end point. <p>This timeout is only required if FortiOS doesn’t receive RADIUS Stop records. However, even if the accounting system does send RADIUS Stop records, this timeout should be set in case the FortiGate unit misses a Stop record.</p> <p>The default timeout is 28800 seconds (8 hours). You can keep this timeout relatively high because its not usually a problem to have a long context list, but entries that are no longer used should be removed regularly. If the timeout is too short, user context entries might be removed prematurely.</p> <p>Set the timeout to 0 if you do not want FortiOS to remove entries from the list except in response to RADIUS Stop messages.</p> | 28800 |

| Variable | Description | Default |
|---|--|--|
| rsso-endpoint-attribute <RADIUS_attribute> | To extract the user end point identifier from the RADIUS Start record, this field must be set to the name of the RADIUS attribute that contains the end point identifier. You can select the <code>RADIUS_attribute</code> from the list or enter an attribute name. The <code>RADIUS_attribute</code> must match one of the RADIUS attributes in the list. The <code>RADIUS_attribute</code> is case sensitive. | Calling-Station-Id |
| rsso-endpoint-block-attribute <RADIUS_attribute> | This field specifies a RADIUS attribute that can be used to block a user. If the attribute value is "Block", FortiOS blocks all traffic from the user's IP address. | Called-Station-Id |
| rsso-flush-ip-session {enable disable} | Enable to flush user IP sessions on RADIUS accounting stop messages. | disable |
| rsso-log-flags <lflags> | <p>Enter one or more of the following options to configure FortiOS to write event log messages for RADIUS SSO events. You can enter multiple options. Separate the options with a space.</p> <p><code>none</code> — Disable logging of RADIUS SSO events.</p> <p><code>accounting-event</code> — Enable to write an event log message when FortiOS does not find the expected information in a RADIUS Record. For example, if a RADIUS record contains more than the expected number of addresses.</p> <p><code>accounting-stop-missed</code> — Enable to write an event log message whenever a user context entry timeout expires indicating that FortiOS removed an entry from the user context list without receiving a RADIUS Stop message.</p> <p><code>context-missing</code> — Enable to write an event log message whenever a user context creation timeout expires indicating that FortiOS was not able to match a communication session because a matching entry was not found in the user context list.</p> <p><code>endpoint-block</code> — Enable to write an event log message whenever a user is blocked because the attribute specified in <code>rsso-endpoint-block-attribute</code> has the value "Block".</p> <p><code>profile-missing</code> — Enable to write an event log message whenever FortiOS cannot find a group name in a RADIUS start message that matches the name of an RSSO user group in FortiOS.</p> <p><code>protocol-error</code> — Enable to write an event log message if RADIUS protocol errors occur. For example, if a RADIUS record contains a RADIUS secret that does not match the one added to the dynamic profile.</p> <p><code>radiusd-other</code> — Enable to write event log messages for other events. The event is described in the log message. For example, write a log message if the memory limit for the user context list is reached and the oldest entries in the table have been dropped.</p> | All options except <code>none</code> . |

| Variable | Description | Default |
|---|---|-------------|
| rsso-log-period <log_time> | The time in seconds to group event log messages for dynamic profile events. For example, if the log message period is 30 seconds, FortiOS Carrier generates groups of event log messages every 30 seconds instead of generating event log messages continuously. And the log messages generated each period contain a count of how many events of that type occurred. If set to 0, FortiOS Carrier generates all event log messages in real time. | 0 |
| rsso-radius-response {enable disable} | Enable if you want FortiOS Carrier to send RADIUS responses after receiving RADIUS Start and Stop records. This setting may be required by your accounting system. | disable |
| rsso-radius-server-port <RADIUS_listen_port> | If required, change the UDP port number used by the RADIUS accounting server for sending RADIUS records. FortiOS Carrier listens for RADIUS Start and Stop records on this port. | 1813 |
| rsso-secret <server_password> | Enter the RADIUS secret used by the RADIUS accounting server. | No default |
| rsso-validate-request-secret {enable disable} | Enable if you want FortiOS Carrier to verify that the RADIUS secret matches the RADIUS secret in the RADIUS Start or End record. You can verify the RADIUS secret to verify that the RADIUS record is valid. | disable |
| sso-attribute <RADIUS_attribute> | To extract a profile group name from the RADIUS Start record, this field must be set to the name of the RADIUS attribute that contains the profile group name. You can select the RADIUS_attribute from the list or enter an attribute name. The RADIUS_attribute must match one of the RADIUS attributes in the list. The RADIUS_attribute is case sensitive. | Class |
| sso-attribute-key <profile_attribute_key> | Enter a string if the profile attribute contains more data than just the profile group name. The profile key is a text string that always comes directly before the profile group name in the profile attribute. For example, if the profile group name always follows the text string profile, the class attribute could include the string: profile=<profile_name_str>. Where <profile_name_str> is the name of the profile group. Maximum 36 characters. | No default. |

setting

Use this command to change per VDOM user settings such as the firewall user authentication time out and protocol support for firewall policy authentication.

user settings differ from system global settings in that system global settings fields apply to the entire FortiGate unit, where user settings fields apply only to the user VDOM.

Syntax

```
config user setting
    set auth-blackout-time <blackout_time_int>
    set auth-cert <cert_name>
    set auth-http-basic {enable | disable}
    set auth-invalid-max <int>
    set auth-lockout-duration <seconds>
    set auth-lockout-threshold <int>
    set auth-multi-group {enable | disable}
    set auth-secure-http {enable | disable}
    set auth-type {ftp | http | https | telnet}
    set auth-timeout <auth_timeout_minutes>
    set auth-timeout-type {idle-timeout | hard-timeout | new-session}
    config auth-ports
        edit <auth-table-entry-id>
            set port <port_int>
            set type {ftp | http | https | telnet}
        end
    end
end
```

| Variable | Description | Default |
|---|--|-----------|
| auth-blackout-time <blackout_time_int> | When a firewall authentication attempt fails 5 times within one minute the IP address that is the source of the authentication attempts is denied access for the <blackout_time_int> period in seconds. The range is 0 to 3600 seconds. | 0 |
| auth-cert <cert_name> | HTTPS server certificate for policy authentication. Fortinet_Factory, Fortinet_Firmware (if applicable to your FortiGate unit), and self-sign are built-in certificates but others will be listed as you add them. | self-sign |
| auth-http-basic {enable disable} | Enable or disable support for HTTP basic authentication for identity-based firewall policies. HTTP basic authentication usually causes a browser to display a pop-up authentication window instead of displaying an authentication web page. Some basic web browsers, for example, web browsers on mobile devices, may only support HTTP basic authentication. | disable |
| auth-invalid-max <int> | Enter the maximum number of failed authentication attempts to allow before the client is blocked. Range: 1-100. | 5 |

| Variable | Description | Default |
|--|--|--------------|
| auth-lockout-duration <seconds> | Enter the login lockout period in seconds. The lockout is imposed after too many failed login attempts, set by <code>auth-lockout-threshold</code> . | 0 |
| auth-lockout-threshold <int> | Enter the number of login attempts that trigger a login lockout. Range 1 to 10. | 3 |
| auth-multi-group {enable disable} | This option can be disabled if the Active Directory structure is setup such that users belong to only 1 group for the purpose of firewall authentication. | enable |
| auth-secure-http {enable disable} | Enable to have <code>http</code> user authentication redirected to secure channel - <code>https</code> . | disable |
| auth-type {ftp http https telnet} | Set the user authentication protocol support for firewall policy authentication. User controls which protocols should support the authentication challenge. | |
| auth-timeout <auth_timeout_minutes> | Set the number of minutes before the firewall user authentication timeout requires the user to authenticate again. The maximum <code>authtimeout</code> interval is 1440 minutes (24 hours). To improve security, keep the authentication timeout at the default value of 5 minutes. | 5 |
| auth-timeout-type {idle-timeout hard-timeout new-session} | Set the type of authentication timeout. <code>idle-timeout</code> — applies only to idle session <code>hard-timeout</code> — applies to all sessions <code>new-session</code> — applies only to new sessions | idle-timeout |
| radius-ses-timeout-act {hard-timeout ignore-timeout} | Select how to use RADIUS session timeout: <code>hard-timeout</code> — use RADIUS timeout <code>ignore-timeout</code> — ignore RADIUS timeout | hard-timeout |
| config auth-ports variables | | |
| <auth-table-entry-id> | Create an entry in the authentication port table if you are using non-standard ports. | |
| port <port_int> | Specify the authentication port. Range 1 to 65535. | 1024 |
| type {ftp http https telnet} | Specify the protocol to which port applies. | http |

tacacs+

Use this command to add or edit the information used for TACACS+ authentication.

Terminal Access Controller Access-Control System (TACACS+) is a remote authentication protocol used to communicate with an authentication server. TACACS+ allows a client to accept a user name and password and send a query to a TACACS+ authentication server. The server host determines whether to accept or deny the request and sends a response back that allows or denies network access to the user.

The default port for a TACACS+ server is 49. The maximum number of remote TACACS+ servers that can be configured for authentication is 10.

You may select an alternative authentication method for each server. These include CHAP, PAP, MS-CHAP, and ASCII.

Syntax

```
config user tacacs+
  edit <server_name>
    set authen-type {ascii | auto | chap | ms_chap | pap}
    set authorization {enable | disable}
    set key <server_key>
    set port <tacacs+_port_num>
    set server <domain>
    set source-ip <ipv4_addr>
  end
```

| Variable | Description | Default |
|---|---|-------------|
| edit <server_name> | Enter a name to identify the TACACS+ server. Enter a new name to create a new server definition or enter an existing server name to edit that server definition. | |
| authen-type {ascii auto chap ms_chap pap} | Select the authentication method for this TACACS+ server. auto uses pap, ms_chap_v, and chap, in that order. | auto |
| authorization {enable disable} | Enable or disable TACACS+ authorization. | disable |
| key <server_key> | Enter the key to access the server. The maximum number is 16. | |
| port <tacacs+_port_num> | Change the default TACACS+ port for this server. The default port for TACACS+ traffic is 49. Range is 0..65535. | 49 |
| server <domain> | Enter the TACACS+ server domain name or IP address. The host name must comply with RFC1035. | No default. |
| source-ip <ipv4_addr> | Enter the source IP for communications to TACACS+ server. | 0.0.0.0 |

•

voip

Use VoIP commands to configure VoIP profiles for firewall policies.

This chapter describes the following command:

[profile](#)

profile

Use this command to add VoIP profiles for SIP, SIMPLE, and SCCP. To apply the SIP ALG, you add a VoIP profile to a firewall policy that accepts SIP sessions. All SIP sessions accepted by the firewall policy will be processed by the SIP ALG using the settings in the VoIP profile. The VoIP profile contains settings that are applied to SIP, Session Initiation Protocol for Instant Messaging and Presence Leveraging Extensions (SIMPLE) and Skinny Call Control Protocol (SCCP) sessions. You configure SIP and SCCP settings separately. SIP settings also apply to SIMPLE sessions.

Syntax

```
config voip profile
  edit <profile_name>
    set comment <comment_str>
    set extended-utm-log {enable | disable}
  config sip
    set status {enable | disable}
    set rtp {enable | disable}
    set open-register-pinhole {enable | disable}
    set open-contact-pinhole {enable | disable}
    set open-record-route-pinhole {enable | disable}
    set open-via-pinhole {enable | disable}
    set strict-register {enable | disable}
    set register-rate <rate_sec_policy_int>
    set invite-rate <rate_sec_policy_int>
    set max-dialogs <max_int>
    set max-line-length <length_int>
    set block-long-lines {enable | disable}
    set block-unknown {enable | disable}
    set call-keepalive <keepalive_time>
    set block-ack {enable | disable}
    set block-bye {enable | disable}
    set block-cancel {enable | disable}
    set block-info {enable | disable}
    set block-invite {enable | disable}
    set block-message {enable | disable}
    set block-notify {enable | disable}
    set block-options {enable | disable}
    set block-prack {enable | disable}
    set block-publish {enable | disable}
    set block-refer {enable | disable}
    set block-register {enable | disable}
    set block-subscribe {enable | disable}
    set block-update {enable | disable}
    set reg-diff-port {enable | disable}
    set rfc2543-branch {enable | disable}
    set log-violations {enable | disable}
    set log-call-summary {enable | disable}
    set nat-trace {enable | disable}
```



```
set subscribe-rate <rate_sec_policy_int>
set message-rate <rate_sec_policy_int>
set notify-rate <rate_sec_policy_int>
set refer-rate <rate_sec_policy_int>
set update-rate <rate_sec_policy_int>
set options-rate <rate_sec_policy_int>
set ack-rate <rate_sec_policy_int>
set prack-rate <rate_sec_policy_int>
set info-rate <rate_sec_policy_int>
set publish-rate <rate_sec_policy_int>
set bye-rate <rate_sec_policy_int>
set cancel-rate <rate_sec_policy_int>
set preserve-override {enable | disable}
set no-sdp-fixup {enable | disable}
set contact-fixup {enable | disable}
set max-idle-dialogs <dialogs_perpolicy_int>
set block-geo-red-options {enable | disable}
set hosted-nat-traversal {enable | disable}
set hnt-restrict-source-ip {enable | disable}
set max-body-length <size_bytes_int>
set unknown-header {discard | pass | respond}
set malformed-request-line {discard | pass | respond}
set malformed-header-via {discard | pass | respond}
set malformed-header-from {discard | pass | respond}
set malformed-header-to {discard | pass | respond}
set malformed-header-call-id {discard | pass | respond}
set malformed-header-cseq {discard | pass | respond}
set malformed-header-rack {discard | pass | respond}
set malformed-header-rseq {discard | pass | respond}
set malformed-header-contact {discard | pass | respond}
set malformed-header-record-route {discard | pass | respond}
set malformed-header-route {discard | pass | respond}
set malformed-header-expires {discard | pass | respond}
set malformed-header-content-type {discard | pass | respond}
set malformed-header-content-length {discard | pass |
    respond}
set malformed-header-max-forwards {discard | pass | respond}
set malformed-header-allow {discard | pass | respond}
set malformed-header-p-asserted-identity {discard | pass |
    respond}
set malformed-header-sdp-v {discard | pass | respond}
set malformed-header-sdp-o {discard | pass | respond}
set malformed-header-sdp-s {discard | pass | respond}
set malformed-header-sdp-i {discard | pass | respond}
set malformed-header-sdp-c {discard | pass | respond}
set malformed-header-sdp-b {discard | pass | respond}
set malformed-header-sdp-z {discard | pass | respond}
set malformed-header-sdp-k {discard | pass | respond}
set malformed-header-sdp-a {discard | pass | respond}
```

```

set malformed-header-sdp-t {discard | pass | respond}
set malformed-header-sdp-r {discard | pass | respond}
set malformed-header-sdp-m {discard | pass | respond}
set ips-rtp {enable | disable}
set provisional-invite-expiry-time <time_int>
set ssl-mode {off | full}
set ssl-algorithm {high | medium | low}
set ssl-auth-client <peer_group>
set ssl-auth-server <peer_group>
set ssl-client-certificate <cert_name>
set ssl-client-renegotiation {allow | deny | secure}
set ssl-min-version {ssl-3.0 | tls-1.0 | tls-1.1}
set ssl-max-version {ssl-3.0 | tls-1.0 | tls-1.1}
set ssl-pfs {require | allow | deny}
set ssl-send-empty-frags {enable | disable}
set ssl-server-certificate <cert_name>
end
config sccp
set status {disable | enable}
set block-mcast {enable | disable}
set verify-header {enable | disable}
set log-call-summary {disable | enable}
set log-violations {disable | enable}
set max-calls <calls_int>
end
end

```

| Variable | Description | Default |
|--|--|---------|
| edit <profile_name> | Enter the name of a VoIP profile | |
| comment <comment_str> | Optionally enter a description of up to 63 characters of the VoIP profile. | |
| extended-utm-log {enable disable} | Enable or disable detailed UTM log messages. | disable |

config sip

Configure VoIP profile settings for SIP and SIMPLE.

| Variable | Description | Default |
|---|--|---------|
| status {enable disable} | Enable or disable SIP for this VoIP profile. | enable |
| rtp {enable disable} | Enable or disable opening pinholes for RTP traffic to traverse FortiGate unit. | enable |
| open-register-pinhole {enable disable} | Enable or disable opening a pinhole for the port number specified in SIP REGISTER message Contact header line. | enable |
| open-contact-pinhole {enable disable} | Enable or disable opening a pinhole for the port number specified in a Contact header line in any SIP message except a SIP REGISTER message. | enable |
| open-record-route-pinhole {enable disable} | Open firewall pinhole for Record-Route port. | enable |

| Variable | Description | Default |
|--|---|---------|
| open-via-pinhole { enable disable } | Open firewall pinhole for Via port. | disable |
| strict-register { enable disable } | Controls how pinholes are opened to allow traffic from a SIP server to pass through the FortiGate unit. If enabled the SIP ALG opens a pinhole that only accepts sessions from a single IP address (the address of the SIP server). This option should be disabled if the SIP proxy server and SIP registrar are different entities with different IP addresses. | disable |
| register-rate <rate_sec_policy_int> | Set a rate limit (per second, per policy) for SIP REGISTER requests. Set to 0 to disable rate limiting. | 0 |
| invite-rate <rate_sec_policy_int> | Set a rate limit (per second, per policy) for SIP INVITE requests. Set to 0 to disable rate limiting. | 0 |
| max-dialogs <max_int> | Maximum number of concurrent calls (or dialogs) per policy. Set to 0 to not limit dialogs. | 0 |
| max-line-length <length_int> | Maximum SIP header line length. The range is 78-4096 characters. If a SIP message contains a line that exceeds the maximum line length a log message is recorded. If <code>block-long-lines</code> is enabled the message is blocked and the FortiGate unit returns a SIP 413 Request entity too large SIP response message. | 998 |
| block-long-lines { enable disable } | Enable or disable blocking SIP request messages with a header or body line that exceeds the <code>max-line-length</code> . | enable |
| block-unknown { enable disable } | Block unrecognized SIP request messages. | enable |
| call-keepalive <keepalive_time> | Continue tracking calls with no RTP sessions for this many minutes. Terminate the call if the time limit is exceeded. Range is 1 and 10,080 seconds. Set to 0 to disable. Call keep alive should be used with caution because enabling this feature results in extra FortiGate CPU overhead and can cause delay/jitter for the VoIP call. Also, the FortiGate unit terminates the call without sending SIP messages to end the call. And if the SIP endpoints send SIP messages to terminate the call they will be blocked by the FortiGate unit if they are sent after the FortiGate unit terminates the call. | 0 |
| block-ack { enable disable } | Enable or disable blocking SIP ACK request messages. | disable |
| block-bye { enable disable } | Enable or disable blocking SIP BYE request messages. | disable |
| block-cancel { enable disable } | Enable or disable blocking SIP CANCEL request messages. | disable |
| block-info { enable disable } | Enable or disable blocking SIP INFO request messages. | disable |
| block-invite { enable disable } | Enable or disable blocking SIP INVITE request messages. | disable |
| block-message { enable disable } | Enable or disable blocking SIP MESSAGE request messages. | disable |
| block-notify { enable disable } | Enable or disable blocking SIP NOTIFY request messages. | disable |

| Variable | Description | Default |
|--|---|---------|
| block-options { enable disable } | Enable or disable blocking SIP OPTIONS request messages. | disable |
| block-prack { enable disable } | Enable or disable blocking SIP PRACK request messages. | disable |
| block-publish { enable disable } | Enable or disable blocking SIP PUBLISH request messages. | disable |
| block-refer { enable disable } | Enable or disable blocking SIP REFER request messages. | disable |
| block-register { enable disable } | Enable or disable blocking SIP REGISTER request messages. | disable |
| block-subscribe { enable disable } | Enable or disable blocking SIP SUBSCRIBE request messages. | disable |
| block-update { enable disable } | Enable or disable blocking SIP UPDATE request messages. | disable |
| reg-diff-port { enable disable } | Enable or disable opening a pinhole for the port number included in the Via SIP message header line. | disable |
| rfc2543-branch { enable disable } | Enable to support RFC 2543-complaint SIP calls involving branch commands that are missing or that are valid for RFC 2543 but invalid for RFC 3261. RFC 3261 is the most recent SIP RFC. RFC 3261 obsoletes RFC 2543. This option also allows FortiGate units to support SIP calls that include Via headers that are missing the branch parameter. | disable |
| log-violations { enable disable } | Enable or disable writing a logging message when a SIP option in a VoIP profile detects a violation in a SIP message. | disable |
| log-call-summary { enable disable } | Enable or disable summary content archiving of SIP calls. | enable |
| nat-trace {enable disable} | Enable or disable preserving the original source IP address of the SIP message in the i= line of the SDP profile. This option enables NAT with IP address conservation (also called SIP NAT tracing), which changes the contents of SIP messages by adding the source IP address of the originator of the message into the SDP i= line of the SIP message. The SDP i= line is used for free-form text. However, if your SIP server can retrieve information from the SDP i= line, it can be useful for keeping a record of the source IP address of the originator of a SIP message when operating in a NAT environment. You can use this feature for billing purposes by extracting the IP address of the originator of the message. | enable |
| subscribe-rate <rate_sec_policy_int> | Limit the number of SIP SUBSCRIBE messages per second per policy that the FortiGate unit accepts. Set to 0 to disable rate limiting. | 0 |
| message-rate <rate_sec_policy_int> | Limit the number of SIP MESSAGE messages per second per policy that the FortiGate unit accepts. Set to 0 to disable rate limiting. | 0 |

| Variable | Description | Default |
|---|---|---------|
| notify-rate <rate_sec_policy_int> | Limit the number of SIP NOTIFY messages per second per policy that the FortiGate unit accepts. Set to 0 to disable rate limiting. | 0 |
| refer-rate <rate_sec_policy_int> | Limit the number of SIP REFER messages per second per policy that the FortiGate unit accepts. Set to 0 to disable rate limiting. | 0 |
| update-rate <rate_sec_policy_int> | Limit the number of SIP UPDATE messages per second per policy that the FortiGate unit accepts. Set to 0 to disable rate limiting. | 0 |
| options-rate <rate_sec_policy_int> | Limit the number of SIP OPTIONS messages per second per policy that the FortiGate unit accepts. Set to 0 to disable rate limiting. | 0 |
| ack-rate <rate_sec_policy_int> | Limit the number of SIP ACK messages per second per policy that the FortiGate unit accepts. Set to 0 to disable rate limiting. | 0 |
| prack-rate <rate_sec_policy_int> | Limit the number of SIP PRACK messages per second per policy that the FortiGate unit accepts. Set to 0 to disable rate limiting. | 0 |
| info-rate <rate_sec_policy_int> | Limit the number of SIP INFO messages per second per policy that the FortiGate unit accepts. Set to 0 to disable rate limiting. | 0 |
| publish-rate <rate_sec_policy_int> | Limit the number of SIP PUBLISH messages per second per policy that the FortiGate unit accepts. Set to 0 to disable rate limiting. | 0 |
| bye-rate <rate_sec_policy_int> | Limit the number of SIP BYE messages per second per policy that the FortiGate unit accepts. Set to 0 to disable rate limiting. | 0 |
| cancel-rate <rate_sec_policy_int> | Limit the number of SIP CANCEL messages per second per policy that the FortiGate unit accepts. Set to 0 to disable rate limiting. | 0 |
| preserve-override {enable disable} | Enable or disable adding the original o= line of a SIP message to the end of the i= line or replace the i= line in the original message with a new i= line. This command is used for SIP IP address conservation. | disable |
| no-sdp-fixup {enable disable} | Enable or disable not performing NAT on addresses in the SDP lines of the SIP message body. This option is disabled by default and the FortiGate unit performs NAT on addresses in SDP lines. Enable this option if you don't want the FortiGate unit to perform NAT on the addresses in SDP lines. | disable |
| contact-fixup {enable disable} | Enable or disable performing NAT on the IP addresses and port numbers in the headers in SIP CONTACT messages even if they don't match the session's IP address and port numbers. | enable |

| Variable | Description | Default |
|--|--|---------|
| max-idle-dialogs <dialogs_perpolicy_int> | Specify the maximum number of established but idle dialogs to retain (per policy). Set to 0 to disable. Idle dialogs would usually be dialogs that have been interrupted because of errors or problems or as the result of a SIP attack that opens a large number of SIP dialogs without closing them. This command provides a way to remove these dialogs from the dialog table and recover memory and resources being used by these open and idle dialogs. | 0 |
| block-geo-red-options {enable disable} | Block OPTIONS requests, but OPTIONS requests still notify for redundancy. | disable |
| hosted-nat-traversal {enable disable} | Enable or disable support for hosted NAT Traversal (HNT). HNT has different requirements for address translation. | disable |
| hnt-restrict-source-ip {enable disable} | Restrict RTP source IP to be the same as SIP source IP when HNT is enabled. | disable |
| max-body-length <size_bytes_int> | Specify the maximum size of a SIP message body in bytes that will be processed by the SIP ALG. Larger messages are discarded. Set to 0 for no limit. This option checks the value in the SIP Content-Length header line to determine body length. The Content-Length can be larger than the actual size of a SIP message if the SIP message content is split over more than one packet. SIP messages are of variable size and the message size can change with the addition of Via and Record-Route headers. | 0 |
| unknown-header {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message with an unknown header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-request-line {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed request-line (the first line in a SIP request message). Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-header-via {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed Via header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-header-from {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed From header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |

| Variable | Description | Default |
|---|--|---------|
| malformed-header-to {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed To header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-header-call-id {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed Call ID header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-header-cseq {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed CSeq header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-header-rack {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed Rack header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-header-rseq {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed RSeq header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-header-contact {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed Contact header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-header-record-route {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed Record-Route header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-header-route {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed Route header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |

| Variable | Description | Default |
|---|---|---------|
| malformed-header-expires {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed Expires header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-header-content-type {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed Content-Type header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-header-content-length {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed Content-Length header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-header-max-forwards {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed Max-forwards header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-header-allow {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed Allow header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-header-p-asserted-identity {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed P-Asserted-Identity header line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-header-sdp-v {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed v= body line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-header-sdp-o {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed o= body line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |

| Variable | Description | Default |
|--|--|---------|
| malformed-header-sdp-s {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed s= body line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-header-sdp-i {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed i= body line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-header-sdp-c {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed c= body line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-header-sdp-b {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed b= body line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-header-sdp-z {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed z= body line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-header-sdp-k {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed k= body line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-header-sdp-a {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed a= body line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-header-sdp-t {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed t= body line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |

| Variable | Description | Default |
|---|---|---------|
| malformed-header-sdp-r {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed r= body line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| malformed-header-sdp-m {discard pass respond} | Configure deep SIP message inspection to discard, pass without changing, or discard and send a SIP response message for a SIP message a with a malformed m= body line. Even if set to pass the SIP ALG writes a log message if an unknown header is found and log-violations is enabled. | pass |
| ips-rtp {enable disable} | Enable to have RTP traffic inherit the IPS setting from the SIP firewall policy. Disable if IPS slows down RTP traffic, which might occur if there is a high volume of RTP traffic. Also if the traffic is using NP accelerated interfaces, enabling IPS means that the RTP traffic cannot be accelerated by NP interface acceleration. | enable |
| provisional-invite-expiry-time <time_int> | The expiry time in seconds to wait for provisional INVITE requests. The range is 10-3600 seconds. | 210 |
| ssl-mode {off full} | Select SSL mode: full — client-to-FortiGate and FortiGate-to-client off — no SSL | off |
| ssl-algorithm {high medium low} | Select SSL algorithm strength: high — AES or 3DES medium — AES, 3DES, RC4, or DES low — AES, 3DES, or RC4 | high |
| ssl-auth-client <peer_group> | Require a client certificate and authenticate it with the peer or peergrp. | null |
| ssl-auth-server <peer_group> | Authenticate the server certificate with the peer or peergrp. | null |
| ssl-client-certificate <cert_name> | Select the certificate to use for client authentication. | null |
| ssl-client-renegotiation {allow deny secure} | Select the client renegotiation policy: allow — allow SSL client to renegotiate deny — reject any attempt to renegotiate secure — reject any renegotiation attempt that does not offer a RFC 5746 Secure Renegotiation Indication | allow |
| ssl-min-version {ssl-3.0 tls-1.0 tls-1.1} | Select the minimum SSL/TLS version to accept. | ssl-3.0 |
| ssl-max-version {ssl-3.0 tls-1.0 tls-1.1} | Select the maximum SSL/TLS version to accept. | tls-1.1 |
| ssl-pfs {require allow deny} | Set policy for Perfect Forward Secrecy (PFS). | allow |

| Variable | Description | Default |
|--|--|---------|
| ssl-send-empty-frags { enable disable } | Enable sending empty fragments to avoid attack on CBC IV (SSL 3.0 & TLS 1.0 only). | enable |
| ssl-server-certificate <cert_name> | Select the certificate to use for server authentication. | null |

config sccp

Configure VoIP profile settings for SCCP.

| Variable | Description | Default |
|---------------------------------------|--|---------|
| status { disable enable } | Enable or disable SCCP. | enable |
| block-mcast { enable disable } | Enable or disable blocking multicast RTP connections. | disable |
| verify-header { enable disable } | Enable or disable verifying SCCP header content. | disable |
| log-call-summary { disable enable } | Enable or disable summary content archiving of SCCP calls. | enable |
| log-violations { disable enable } | Enable or disable writing a logging message when a SIP option in a VoIP profile detects a violation in a SIP message. | disable |
| max-calls <calls_int> | Enter the maximum number of calls per minute per SCCP client. The range is 1 to 65535. Set to 0 to disable limiting the number of calls. | 0 |

vpn

Use `vpn` commands to configure options related to virtual private networking through the FortiGate unit, including:

- IPsec operating parameters
- a local address range for PPTP or L2TP clients
- SSL VPN configuration settings

This chapter contains the following sections:

| | |
|---|--|
| certificate ca | l2tp |
| certificate crt | pptp |
| certificate local | ssl settings |
| certificate ocsf-server | ssl web host-check-software |
| certificate remote | ssl web portal |
| certificate setting | ssl web realm |
| ipsec concentrator | ssl web user |
| ipsec forticlient | ssl web virtual-desktop-app-list |
| ipsec manualkey | |
| ipsec manualkey-interface | |
| ipsec phase1 | |
| ipsec phase1-interface | |
| ipsec phase2 | |
| ipsec phase2-interface | |

certificate ca

Use this command to install Certificate Authority (CA) root certificates.

When a CA processes your Certificate Signing Request (CSR), it sends you the CA certificate, the signed local certificate and the Certificate Revocation List (CRL).

The process for obtaining and installing certificates is as follows:

1. Use the `execute vpn certificate local` command to generate a CSR.
2. Send the CSR to a CA.
The CA sends you the CA certificate, the signed local certificate and the CRL.
3. Use the `vpn certificate local` command to install the signed local certificate.
4. Use the `vpn certificate ca` command to install the CA certificate.
5. Use the `vpn certificate crl` command to install the CRL.

Depending on your terminal software, you can copy the certificate and paste it into the command.

The CA certificate can update automatically from a Simple Certificate Enrollment Protocol (SCEP) server.

Syntax

```
config vpn certificate ca
  edit <ca_name>
    set ca <cert>
    set auto-update-days <days_int>
    set auto-update-days-warning <days_int>
    set scep-url <URL_str>
    set source-ip <ip4_addr>
  end
```

To view all of the information about the certificate, use the `get` command:

```
get vpn certificate ca <ca_name>
```

| Variable | Description | Default |
|--|--|-------------|
| edit <ca_name> | Enter a name for the CA certificate. | No default. |
| ca <cert> | Enter or retrieve the CA certificate in PEM format. | No default. |
| Fields relevant to SCEP auto-update | | |
| auto-update-days <days_int> | Enter how many days before expiry the FortiGate unit requests an updated CA certificate. Enter 0 for no auto-update. | 0 |
| auto-update-days-warning <days_int> | Enter how many days before CA certificate expiry the FortiGate generates a warning message. Enter 0 for no warning. | 0 |
| scep-url <URL_str> | Enter the URL of the SCEP server. | No default. |
| source-ip <ip4_addr> | Enter an address to verify request is send from expected IP. <code>source-ip</code> can be set after local Certificate is generated. | No default. |

certificate crl

Use this command to install a Certificate Revocation List (CRL).

When a CA processes your Certificate Signing Request (CSR), it sends you the CA certificate, the signed local certificate and the Certificate Revocation List (CRL).

The process for obtaining and installing certificates is as follows:

1. Use the `execute vpn certificate local` command to generate a CSR.
2. Send the CSR to a CA.
The CA sends you the CA certificate, the signed local certificate and the CRL.
3. Use the `vpn certificate local` command to install the signed local certificate.
4. Use the `vpn certificate ca` command to install the CA certificate.
5. Use the `vpn certificate crl` command to install the CRL.

Depending on your terminal software, you can copy the certificate and paste it into the command.

The CRL can update automatically from a Simple Certificate Enrollment Protocol (SCEP) server.

Syntax

```
config vpn certificate crl
  edit <crl_name>
    set crl <crl_PEM>
    set ldap-server <ldap_server_name>
    set ldap-username <ldap_username>
    set ldap-password <ldap_password>
    set scep-cert <scep_certificate>
    set scep-url <scep_url>
    set source-ip <ip4_addr>
    set update-vdom <update_vdom>
    set http-url <http_url>
    set update-interval <seconds>
  end
```

| Variable | Description | Default |
|---|--|-------------------|
| <code>edit <crl_name></code> | Enter a name for the Certificate Revocation List (CRL). | |
| <code>crl <crl_PEM></code> | Enter the CRL in PEM format. | |
| <code>ldap-server <ldap_server_name></code> | Name of the LDAP server defined in config user ldap table for CRL auto-update. | |
| <code>ldap-username <ldap_username></code> | LDAP login name. | |
| <code>ldap-password <ldap_password></code> | LDAP login password. | |
| <code>scep-cert <scep_certificate></code> | Local certificate used for SCEP communication for CRL auto-update. | Fortinet-Firmware |
| <code>scep-url <scep_url></code> | URL of the SCEP server used for automatic CRL certificate updates. The URL must begin with <code>http://</code> or <code>https://</code> . | |
| <code>source-ip <ip4_addr></code> | Enter an address to verify request is send from expected IP. <code>source-ip</code> can be set after local Certificate is generated. | No default. |

| Variable | Description | Default |
|------------------------------|---|---------|
| update-vdom <update_vdom> | VDOM used to communicate with remote SCEP server for CRL auto-update. | root |
| http-url <http_url> | URL of an http server used for automatic CRL certificate updates. The URL must begin with <code>http://</code> or <code>https://</code> . | |
| update-interval <seconds> | Enter how frequently, in seconds, the FortiGate unit checks for an updated CRL. Enter 0 to update the CRL only when it expires. This option is available when you add a <code>scep-url</code> . | |

certificate local

Use this command to install local certificates.

When a CA processes your Certificate Signing Request (CSR), it sends you the CA certificate, the signed local certificate and the Certificate Revocation List (CRL).

The process for obtaining and installing certificates is as follows:

1. Use the `execute vpn certificate local` command to generate a CSR.
2. Send the CSR to a CA.
The CA sends you the CA certificate, the signed local certificate and the CRL.
3. Use the `vpn certificate local` command to install the signed local certificate.
4. Use the `vpn certificate ca` command to install the CA certificate.
5. Use the `vpn certificate crl` command to install the CRL.

Depending on your terminal software, you can copy the certificate and paste it into the command.

The local certificate can update automatically from a Simple Certificate Enrollment Protocol (SCEP) server.

Syntax

```
config vpn certificate local
  edit <cert_name>
    set password <pwd>
    set comments <comment_text>
    set private-key <prkey>
    set source-ip <ip4_addr>
    set certificate <cert_PEM>
    set csr <csr_PEM>
    set scep-url <URL_str>
    set scep-password <password_str>
    set auto-regenerate-days <days_int>
    set auto-regenerate-days-warning <days_int>
  end
```

To view all of the information about the certificate, use the `get` command:

```
get vpn certificate local [cert_name]
```

| Variable | Description | Default |
|---|--|-------------|
| edit <cert_name> | Enter the local certificate name. | No default. |
| certificate <cert_PEM> | Enter the signed local certificate in PEM format. | No default. |
| comments <comment_text> | Enter any relevant information about the certificate. | No default. |
| You should not modify the following variables if you generated the CSR on this unit. | | |
| csr <csr_PEM> | The CSR in PEM format. | No default. |
| password <pwd> | The password in PEM format. | No default. |
| private-key <prkey> | The private key in PEM format. | No default. |
| source-ip <ip4_addr> | Enter an address to verify request is send from expected IP. <code>source-ip</code> can be set after local Certificate is generated. | No default. |

| Variable | Description | Default |
|---|---|-------------|
| Fields relevant to SCEP auto-update | | |
| scep-url <URL_str> | Enter the URL of the SCEP server. | No default. |
| scep-password <password_str> | Enter the password for the SCEP server. | No default. |
| auto-regenerate-days <days_int> | Enter how many days before expiry the FortiGate unit requests an updated local certificate. Enter 0 for no auto-update. | 0 |
| auto-regenerate-days- warning <days_int> | Enter how many days before local certificate expiry the FortiGate generates a warning message. Enter 0 for no warning. | 0 |

certificate ocsdp-server

Use this command to specify the revocation server for an OCSdp (Online Certificate Status Protocol) server certificate. You can also specify the action to take if the server is not available.

Syntax

```
config vpn certificate ocsdp-server
edit <ocsp_name>
set cert <cert_name>
set secondary-cert <cert2_name>
set secondary-url <ocsp2_url>
set source-ip <ip4_addr>
set url <ocsp_url>
set unavail-action <unavailable_action>
end
```

To view all of the information about the certificate, use the `get` command:

```
get vpn certificate ocsdp [cert_name]
```

| Variable | Description |
|-------------------------------------|--|
| <ocsp_name> | Enter a name for this OSCP server entry. |
| cert <cert_name> | Enter the OCSdp server public certificate (one of the remote certificates). |
| secondary-cert <cert2_name> | Enter the secondary OCSdp server public certificate (one of the remote certificates). |
| secondary-url <ocsp2_url> | Enter the URL of the secondary OCSdp server. |
| source-ip <ip4_addr> | Enter an address to verify request is send from expected IP. <i>source-ip</i> can be set after local Certificate is generated. |
| url <ocsp_url> | Enter the URL of the OCSdp server. |
| unavail-action <unavailable_action> | Action taken on client certification when the OCSdp server is unreachable. <i>revoke</i> or <i>ignore</i> . Default is <i>revoke</i> . |

certificate remote

Use this command to install remote certificates. The remote certificates are public certificates without a private key. They are used as OCSP (Online Certificate Status Protocol) server certificates.

Syntax

```
config vpn certificate remote
  edit cert <cert_name>
    set remote <remote_cert_detail>
  end
```

To view all of the information about the certificate, use the `get` command:

```
get vpn certificate remote [cert_name]
```

| Variable | Description |
|-----------------------------|--|
| cert <cert_name> | Enter the name of the public certificate. |
| remote <remote_cert_detail> | Details/description of the remote certificate. |

certificate setting

Use this command to enable obtaining certificates by OSCP.

Syntax

```
config vpn certificate setting
  set check-ca-cert {enable | disable}
  set obsp-status {enable | disable}
  set obsp-default-server <osp_name>
end
```

| Variable | Description | Default |
|-------------------------------------|--|---------|
| check-ca-cert {enable disable} | Enable to check certificate and fail the authentication if the CA certificate is not found. | enable |
| osp-status {enable disable} | Enable or disable obtaining certificates by OSCP | disable |
| osp-default-server <osp_name> | Enter the OSCP server to use by default. This is one of the servers defined in <code>vpn certificate osp-server</code> . | null |

ipsec concentrator

Use this command to add IPsec policy-based VPN tunnels to a VPN concentrator. The VPN concentrator collects hub-and-spoke tunnels into a group.

The concentrator allows VPN traffic to pass from one tunnel to the other through the FortiGate unit. The FortiGate unit functions as a concentrator, or hub, in a hub-and-spoke network.



VPN concentrators are not available in Transparent mode.

Syntax

```
config vpn ipsec concentrator
edit <concentrator_name>
    set member <member_name> [member_name] [member_name]
    set src-check {enable | disable}
end
```

The member field is required.

| Variable | Description | Default |
|---|--|-------------|
| edit <concentrator_name> | Enter a name for the concentrator. | No default. |
| member <member_name> [member_name] [member_name] | Enter the names of up to three VPN tunnels to add to the concentrator. Separate the tunnel names with spaces. Members can be tunnels defined in <code>vpn ipsec phase1</code> or <code>vpn ipsec manual-key</code> . To add or remove tunnels from the concentrator you must re-enter the whole list with the required additions or deletions. | No default. |
| src-check {enable disable} | Enable to check the source address of the phase2 selector when locating the best matching phase2 in a concentrator. The default is to check only the destination selector. | disable |

ipsec forticlient

Use this command to configure automatic VPN configuration for FortiClient Host Security application users.

The FortiClient users who will use automatic configuration must be members of a user group. The `config vpn ipsec forticlient` command creates a “realm” that associates the user group with the phase 2 VPN configuration. You can create multiple realms to associate different user groups with different phase 2 configurations.

The user group identifies the user name and password settings that the dialup client’s credentials must match in order for authentication to be successful. The phase 2 tunnel definition and its associated firewall encryption policy provides the configuration parameters to download to the FortiClient Host Security application.

Syntax

Set or unset VPN policy distribution parameters.

```
config vpn ipsec forticlient
  edit <realm_name>
    set phase2name <tunnel_name>
    set status {enable | disable}
    set usergroupname <group_name>
  end
```

| Variable | Description | Default |
|-------------------------------|---|-------------|
| edit <realm_name> | Enter a name for the FortiClient realm. This is also referred to as the policy name. | No default. |
| phase2name <tunnel_name> | Enter the name of the phase 2 tunnel configuration that you defined as part of the dialup-client configuration. | Null |
| status {enable disable} | Enable or disable IPSec VPN policy distribution. | enable |
| usergroupname <group_name> | Enter the name of the user group that you created for dialup clients. This group must already exist. | Null |

ipsec manualkey

Use this command to configure manual keys for IPSec tunnel-mode VPN tunnels. You configure a manual key tunnel to create an IPSec tunnel-mode VPN tunnel between the FortiGate unit and a remote IPSec VPN client or gateway that is also using manual key.

A manual key VPN tunnel consists of a name for the tunnel, the IP address of the VPN gateway or client at the opposite end of the tunnel, and the encryption and authentication algorithms to use for the tunnel. Because the keys are created when you configure the tunnel, no negotiation is required for the VPN tunnel to start. However, the VPN gateway or client that connects to this tunnel must use the same encryption and authentication algorithms and must have the same encryption and authentication keys.

Syntax

```
config vpn ipsec manualkey
  edit <tunnel_name>
    set authentication <authentication_algorithm>
    set authkey <authentication_key>
    set encryption <method>
    set enckey <encryption_key>
    set interface <interface_name>
    set localspi <local_spi_number>
    set local-gw <address_ipv4>
    set npu-offload {enable | disable}
    set remote-gw <address_ipv4>
    set remotespi <remote_spi_number>
  end
```

The authentication, encryption, interface, remote-gw, localspi, and remotespi fields are required. All other fields are optional.

| Variable | Description | Default |
|--|--|-------------|
| edit <tunnel_name> | Enter a name for the tunnel. | No default. |
| authentication <authentication_algorithm> | <p>Enter one of the following authentication algorithms:</p> <ul style="list-style-type: none">md5nullsha1sha256sha384sha512 <p>Make sure you use the same algorithm at both ends of the tunnel.</p> <p>Note: encryption and authentication cannot both be null.</p> | null |

| Variable | Description | Default |
|---------------------------------|---|------------------------|
| authkey <authentication_key> | <p>This field is available when authentication is set to md5, sha1, or sha256.</p> <p>Enter the key in 16-digit (8-byte) segments separated by hyphens. For example (MD5):</p> <p>0102030405060708-090a0b0c0d0e0f10</p> <p>For a SHA1 key, the final segment is only 8 digits (4 bytes).</p> <ul style="list-style-type: none"> If authentication is md5, enter a 32-digit (16-byte) hexadecimal number. If authentication is sha1, enter a 40-digit (20-byte) hexadecimal number. If authentication is sha256, enter a 64-digit (32-byte) hexadecimal number. <p>Digits can be 0 to 9, and a to f.</p> <p>Use the same authentication key at both ends of the tunnel.</p> | - (No default.) |
| encryption <method> | <p>Enter one of the following encryption algorithms:</p> <ul style="list-style-type: none"> 3des aes128 aes192 aes256 aria128 aria192 aria256 des seed null <p>The ARIA and seed algorithms are not available on some models.</p> <p>Make sure you use the same algorithm at both ends of the tunnel.</p> <p>Note: encryption and authentication cannot both be null.</p> | null |

| Variable | Description | Default |
|-----------------------------------|---|--------------------|
| enckey <encryption_key> | <p>This field is available when encryption is set to 3des, aes128, aes192, aes256, or des. Enter the associated encryption key:</p> <ul style="list-style-type: none"> If encryption is des, enter a 16 digit (8 byte) hexadecimal number. If encryption is 3des, enter a 48 digit (24 byte) hexadecimal number. If encryption is aes128, enter a 32 digit (16 byte) hexadecimal number. If encryption is aes192, enter a 48 digit (24 byte) hexadecimal number. If encryption is aes256, enter a 64 digit (32 byte) hexadecimal number. <p>Digits can be 0 to 9, and a to f.</p> <p>For all of the above, separate each 16 digit (8 byte) hexadecimal segment with a hyphen.</p> <p>Use the same encryption key at both ends of the tunnel.</p> | - (No default.) |
| interface <interface_name> | <p>Enter the name of the physical, aggregate, or VLAN interface to which the IPSec tunnel will be bound. The FortiGate unit obtains the IP address of the interface from system interface settings (see “interface” on page 555).</p> <p>You cannot change interface if a firewall policy references this VPN.</p> | Null. |
| local-gw <address_ipv4> | Optionally, specify a secondary IP address of the interface selected in interface to use for the local end of the VPN tunnel. If you do not specify an IP address here, the FortiGate unit obtains the IP address of the interface from the system interface settings (see “interface” on page 555). | 0.0.0.0 |
| localspi <local_spi_number> | Local Security Parameter Index. Enter a hexadecimal number of up to eight digits (digits can be 0 to 9, a to f) in the range 0x100 to FFFFFFFF. This number must be added to the Remote SPI at the opposite end of the tunnel. | 0x100 |
| npu-offload {enable disable} | Enable or disable offload of VPN session to NPU. | enable |
| remote-gw <address_ipv4> | The IP address of the remote gateway external interface. | 0.0.0.0 |
| remotespi <remote_spi_number> | Remote Security Parameter Index. Enter a hexadecimal number of up to eight digits in the range 0x100 to FFFFFFFF. This number must be added to the Local SPI at the opposite end of the tunnel. | 0x100 |

ipsec manualkey-interface

Use this command to configure manual keys for a route-based (interface mode) IPSec VPN tunnel. When you create a route-based tunnel, the FortiGate unit creates a virtual IPSec interface automatically. The interface can be modified afterward using the `system network interface` CLI command. This command is available only in NAT/Route mode.

Syntax

```
config vpn ipsec manualkey-interface
  edit <tunnel_name>
    set auth-alg <authentication_algorithm>
    set auth-key <authentication_key>
    set enc-alg <method>
    set enc-key <encryption_key>
    set interface <interface_name>
    set ip-version <4 | 6>
    set local-gw <address_ipv4>
    set local-gw6 <address_ipv6>
    set local-spi <local_spi_number>
    set npu-offload {enable | disable}
    set remote-gw <address_ipv4>
    set remote-gw6 <address_ipv6>
    set remote-spi <remote_spi_number>
  end
```

The `auth-alg`, `enc-alg`, `interface`, `remote-gw`, `local-spi`, and `remote-spi` fields are required. All other fields are optional.

| Variable | Description | Default |
|--|---|-------------|
| edit <tunnel_name> | Enter a name for the tunnel. | No default. |
| auth-alg <authentication_algorithm> | Enter one of the following authentication algorithms: <ul style="list-style-type: none">md5nullsha1sha256sha384sha512 Make sure you use the same algorithm at both ends of the tunnel. Note: <code>enc-alg</code> and <code>auth-alg</code> cannot both be null. | null |

| Variable | Description | Default |
|----------------------------------|--|------------------------|
| auth-key <authentication_key> | <p>This field is available when auth-alg is set to md5, sha1 or sha256.</p> <p>Enter the key in 16-digit (8-byte) segments separated by hyphens. For example (MD5):</p> <p>0102030405060708-090a0b0c0d0e0f10</p> <p>For a SHA1 key, the final segment is only 8 digits (4 bytes).</p> <ul style="list-style-type: none"> • If auth-alg is md5, enter a 32-digit (16-byte) hexadecimal number. • If auth-alg is sha1, enter a 40-digit (20-byte) hexadecimal number. • If auth-alg is sha256, enter a 64-digit (32-byte) hexadecimal number. <p>Digits can be 0 to 9, and a to f.</p> <p>Use the same authentication key at both ends of the tunnel.</p> | - (No default.) |
| enc-alg <method> | <p>Enter one of the following encryption algorithms:</p> <ul style="list-style-type: none"> • 3des • aes128 • aes192 • aes256 • des • aria128 • aria192 • aria256 • seed • null <p>The ARIA algorithm is not available on some models.</p> <p>Make sure you use the same algorithm at both ends of the tunnel.</p> <p>Note: enc-alg and auth-alg cannot both be null.</p> | null |

| Variable | Description | Default |
|--|---|------------------------------------|
| enc-key <encryption_key> | <p>This field is available when enc-alg is set to 3des, aes128, aes192, aes256, or des. Enter the associated encryption key:</p> <ul style="list-style-type: none"> If enc-alg is des, enter a 16 digit (8 byte) hexadecimal number. If enc-alg is 3des, enter a 48 digit (24 byte) hexadecimal number. If enc-alg is aes128, enter a 32 digit (16 byte) hexadecimal number. If enc-alg is aes192, enter a 48 digit (24 byte) hexadecimal number. If enc-alg is aes256, enter a 64 digit (32 byte) hexadecimal number. <p>Digits can be 0 to 9, and a to f.</p> <p>For all of the above, separate each 16 digit (8 byte) hexadecimal segment with a hyphen.</p> <p>Use the same encryption key at both ends of the tunnel.</p> | - (No default.) |
| interface <interface_name> | Enter the name of the physical, aggregate, or VLAN interface to which the IPSec tunnel will be bound. The FortiGate unit obtains the IP address of the interface from system interface settings (see “interface” on page 555). | Null. |
| ip-version <4 6> | Enter 4 for IPv4 encapsulation or 6 for IPv6 encapsulation. | 4 |
| local-gw <address_ipv4> local-gw6 <address_ipv6> | <p>By default, the FortiGate unit determines the local gateway IP address from the interface setting. Optionally, you can specify a secondary IP address configured on the same interface.</p> <p>local-gw6 is available when ip-version is 6. local-gw is available when ip-version is 4.</p> | 0.0.0.0 for IPv4 :: for IPv6 |
| local-spi <local_spi_number> | Local Security Parameter Index. Enter a hexadecimal number of up to eight digits (digits can be 0 to 9, a to f) in the range 0x100 to FFFFFFFF. This number must be added to the Remote SPI at the opposite end of the tunnel. | 0x100 |
| npu-offload { enable disable } | Enable or disable offload of VPN session to NPU. | enable |
| remote-gw <address_ipv4> remote-gw6 <address_ipv6> | <p>The IP address of the remote gateway external interface.</p> <p>remote-gw6 is available when ip-version is 6. remote-gw is available when ip-version is 4.</p> | 0.0.0.0 for IPv4 :: for IPv6 |
| remote-spi <remote_spi_number> | Remote Security Parameter Index. Enter a hexadecimal number of up to eight digits in the range 0x100 to FFFFFFFF. This number must be added to the Local SPI at the opposite end of the tunnel. | 0x100 |

ipsec phase1

Use this command to add or edit IPsec tunnel-mode phase 1 configurations. When you add a tunnel-mode phase 1 configuration, you define how the FortiGate unit and a remote VPN peer (gateway or client) authenticate themselves to each other as part of establishing an IPsec VPN tunnel.

The phase 1 configuration specifies the name of a remote VPN peer, the nature of the connection (static IP, dialup, or dynamic DNS), the encryption and authentication keys for the phase 1 proposal, and the authentication method (preshared key or certificate). For authentication to be successful, the FortiGate unit and the remote VPN peer must be configured with compatible phase 1 settings.

You can change all settings except the `type` setting after you define the configuration: if the address type of a remote peer changes, you must delete the original phase 1 configuration and define a new one. As a general rule, create only one phase 1 configuration per remote VPN peer.

Syntax

```
config vpn ipsec phase1
  edit <gateway_name>
    set add-gw-route {enable | disable}
    set authmethod <authentication_method>
    set authpasswd <password>
    set authusr <user_name>
    set authusrgrp <group_name>
    set autoconfig {client | gateway | disable}
    set auto-negotiate {enable | disable}
    set dhgrp {1 2 5 14}
    set distance <int>
    set dpd {disable | enable}
    set dpd-retrycount <retry_integer>
    set dpd-retryinterval <seconds> [<milliseconds>]
    set forticlient-enforcement {enable | disable}
    set fragmentation {enable | disable}
    set ike-version {1 | 2}
    set interface <interface_name>
    set keepalive <seconds>
    set keylife <seconds>
    set local-gw <address_ipv4>
    set localid <local_id>
    set localid-type {auto | fqdn | user-fqdn | keyid | address
      | asn1dn}
    set mode {aggressive | main}
    set nattraversal {enable | disable}
    set negotiate-timeout <seconds_int>
    set peer <CA_certificate_name>
    set peerid <peer_id>
    set peergrp <certificate_group_name>
    set peertype <authentication_method>
    set priority <prio>
    set proposal <encryption_combination>
```

```

set psksecret <preshared_key>
set remote-gw <address_ipv4>
set remotegw-ddns <domain_name>
set rsa-certificate <server_certificate>
set type <remote_gw_type>
set usrgrp <group_name>
set xauthtype <XAuth_type>
set xauthexpire {on-disconnect | on-rekey}
end

```



A proposal value is required. In NAT/Route mode, you must specify interface. A remote-gw value may be required depending on the value of the type attribute. You must also enter a preshared key or a certificate name depending on the value of authmethod. All other fields are optional.

| Variable | Description | Default |
|---------------------------------------|--|-------------|
| edit <gateway_name> | Enter a name (maximum 35 characters) for this gateway. If type is dynamic, the maximum name length is further reduced depending on the number of dialup tunnels that can be established: by 2 for up to 9 tunnels, by 3 for up to 99 tunnels, 4 for up to 999 tunnels, and so on. | No default. |
| add-gw-route {enable disable} | Enable to automatically add a route to the remote gateway specified in remote-gw. Note: This command is deprecated. Use the <code>dynamic-gateway {enable disable}</code> field in config <code>router static</code> instead. | disable |
| authmethod <authentication_method> | Specify the authentication method: <ul style="list-style-type: none"> Enter <code>psk</code> to authenticate using a pre-shared key. Use <code>psksecret</code> to enter the pre-shared key. Enter <code>rsa-signature</code> to authenticate using a digital certificate. Use <code>set rsa-certificate</code> to enter the name of the digital certificate. You must configure certificates before selecting <code>rsa-signature</code> here. For more information, see “execute <code>vpn certificate local</code> ” on page 1006 and “ <code>vpn certificate ca</code> ” on page 757. | psk |
| authpasswd <password> | This field is available when xauthtype is set to client. Enter the XAuth client password for the FortiGate unit. | No default. |
| authusr <user_name> | This field is available when xauthtype is set to client. Enter the XAuth client user name for the FortiGate unit. | Null |

| Variable | Description | Default |
|---|--|---------|
| authusrgrp <group_name> | <p>This field is available when xauthtype is set to auto, pap, or chap.</p> <p>When the FortiGate unit is configured as an XAuth server, enter the user group to authenticate remote VPN peers. The user group can contain local users, LDAP servers, and RADIUS servers. The user group must be added to the FortiGate configuration before the group name can be cross-referenced. For more information, see “user group” on page 722, “user ldap” on page 726, “user local” on page 729, and “user radius” on page 735.</p> | Null |
| autoconfig {client gateway disable} | Select VPN auto configuration mode: VPN gateway, VPN client, or auto configuration disabled. | disable |
| auto-negotiate {enable disable} | Enable to keep trying to negotiate an IKE SA even if the link is down. The primary use of this feature is in cases where there are multiple redundant tunnels and you prefer the primary connection if it can be established. | enable |
| dhgrp {1 2 5 14} | Type 1, 2, 5 and/or 14 to select one or more Diffie-Hellman groups from DH group 1, 2, 5 and 14 respectively. At least one of the DH group settings on the remote peer or client must be identical to one of the selections on the FortiGate unit. | 5 |
| distance <int> | Configure the administrative distance for routes added when a dialup IPsec connection is established. Using administrative distance you can specify the relative priorities of different routes to the same destination. A lower administrative distance indicates a more preferred route. Distance can be an integer from 1-255. See also router static “distance <distances>” on page 447 . | 1 |
| dpd {disable enable} | Enable or disable DPD (Dead Peer Detection). DPD detects the status of the connection between VPN peers. Enabling DPD facilitates cleaning up dead connections and establishing new VPN tunnels. DPD is not supported by all vendors and is not used unless DPD is supported and enabled by both VPN peers. | enable |
| dpd-retrycount <retry_integer> | <p>This field is available when dpd is set to enable.</p> <p>The DPD retry count when dpd is set to enable. Set the number of times that the local VPN peer sends a DPD probe before it considers the link to be dead and tears down the security association (SA). The dpd-retrycount range is 0 to 10.</p> <p>To avoid false negatives due to congestion or other transient failures, set the retry count to a sufficiently high value for your network.</p> | 3 |

| Variable | Description | Default |
|---|--|---------|
| dpd-retryinterval <seconds> [<milliseconds>] | <p>This field is available when <code>dpd</code> is set to <code>enable</code>.</p> <p>The DPD (Dead Peer Detection) retry interval is the time that the local VPN peer waits between sending DPD probes.</p> <p>Set the time in seconds plus, optionally, milliseconds. For example, for 2.5 seconds enter 2 500. The range is 1 to 60 seconds, 0 to 999 milliseconds.</p> <p>When the tunnel is starting, or if it has failed, a retry interval of 5 seconds is used if <code>dpd-retryinterval</code> is less than 5 seconds.</p> | 5 |
| forticlient-enforcement {enable disable} | Enable to allow only FortiClient users to connect. | disable |
| fragmentation {enable disable} | Enable intra-IKE fragmentation support on re-transmission of fragmented packets. | enable |
| ike-version {1 2} | Select whether to use IKEv1 or IKEv2 (RFC 4306). | 1 |
| interface <interface_name> | <p>Enter the name of the physical, aggregate, or VLAN interface to which the IPsec tunnel will be bound. The FortiGate unit obtains the IP address of the interface from system interface settings (see “interface” on page 555) unless you specify a different IP address using the <code>local-gw <address_ipv4></code> attribute.</p> <p>You cannot change <code>interface</code> if a firewall policy references this VPN.</p> | Null |
| keepalive <seconds> | <p>This field is available when <code>nattraversal</code> is set to <code>enable</code>.</p> <p>Set the NAT traversal keepalive frequency. This number specifies (in seconds) how frequently empty UDP packets are sent through the NAT device to make sure that the NAT mapping does not change until P1 and P2 security associations expire. The keepalive frequency can be from 10 to 900 seconds.</p> | 10 |
| keylife <seconds> | Set the keylife time. The keylife is the amount of time (in seconds) before the phase 1 encryption key expires. When the key expires, a new key is generated without interrupting service. The range is 120 to 172,800 seconds. | 28800 |
| local-gw <address_ipv4> | Optionally, specify a secondary IP address of the interface selected in <code>interface</code> to use for the local end of the VPN tunnel. If you do not specify an IP address here, the FortiGate unit obtains the IP address of the interface from the system interface settings (see “interface” on page 555). | 0.0.0.0 |

| Variable | Description | Default |
|---|--|---------|
| localid <local_id> | <p>Enter a local ID if the FortiGate unit is functioning as a VPN client and will use the local ID for authentication purposes.</p> <p>If you want to dedicate a tunnel to a FortiGate dialup client, you must assign a unique identifier (local ID) to the FortiGate client.</p> <p>Whenever you configure a unique identifier (local ID) on a FortiGate dialup client, you must enable aggressive mode on the FortiGate dialup server and also specify the identifier as a peer ID on the FortiGate dialup server.</p> | Null |
| localid-type {auto fqdn user-fqdn keyid address asn1dn} | <p>Select the type of localid:</p> <p>auto — select type automatically</p> <p>fqdn — Fully Qualified Domain Name</p> <p>user-fqdn — Use User Fully Qualified Domain Name</p> <p>keyid — Use Key Identifier ID</p> <p>address — Use IP address ID</p> <p>asn1dn — Use ASN.1 Distinguished Name ID</p> | auto |
| mode {aggressive main} | <p>Enter aggressive or main (ID Protection) mode. Both modes establish a secure channel.</p> <p>In main mode, identifying information is hidden. Main mode is typically used when both VPN peers have static IP addresses.</p> <p>In aggressive mode, identifying information is exchanged in the clear.</p> <p>When the remote VPN peer or client has a dynamic IP address, or the remote VPN peer or client will be authenticated using an identifier (local ID), you must select Aggressive mode if there is more than one dialup phase 1 configuration for the interface IP address.</p> | main |
| natraversal {enable disable} | <p>Enable NAT traversal if you expect the IPSec VPN traffic to go through a gateway that performs NAT. If no NAT device is detected, enabling NAT traversal has no effect. Both ends of the VPN must have the same NAT traversal setting. If you enable NAT traversal you can set the <code>keepalive</code> frequency.</p> | enable |
| negotiate-timeout <seconds_int> | <p>Enter how long in seconds the FortiGate unit will wait for the IKE SA to be negotiated. Range: 1 to 300 seconds.</p> | 30 |

| Variable | Description | Default |
|-------------------------------------|--|---------|
| peer <CA_certificate_name> | <p>This field is available when <code>authmethod</code> is set to <code>rsa-signature</code> and <code>peertype</code> is set to <code>peer</code>.</p> <p>Enter the name of the peer (CA) certificate that will be used to authenticate remote VPN clients or peers. Use the command <code>config user peer</code> to add peer certificates. Peer certificates must be added to the FortiGate configuration before they can be cross-referenced. For more information, see “user peer” on page 732.</p> | Null |
| peerid <peer_id> | <p>This field is available when <code>peertype</code> is set to <code>one</code>.</p> <p>Enter the peer ID that will be used to authenticate remote clients or peers by peer ID.</p> | Null |
| peergrp <certificate_group_name> | <p>This field is available when <code>type</code> is set to <code>dynamic</code>, <code>authmethod</code> is set to <code>rsa-signature</code>, and <code>peertype</code> is set to <code>peergrp</code>.</p> <p>Enter the name of the peer certificate group that will be used to authenticate remote clients or peers. You must create the peer certificate group before the group name can be cross-referenced. For more information, see “user peergrp” on page 734.</p> | Null |
| peertype <authentication_method> | <p>The following attributes are available under the following conditions:</p> <ul style="list-style-type: none"> • <code>one</code> is available when <code>mode</code> is set to <code>aggressive</code> or when <code>authmethod</code> is set to <code>rsa-signature</code>. • <code>dialup</code> is available when <code>type</code> is set to <code>dynamic</code> and <code>authmethod</code> is set to <code>psk</code>. • <code>peer</code> is available when <code>authmethod</code> is set to <code>rsa-signature</code>. • <code>peergrp</code> is available when <code>type</code> is set to <code>dynamic</code> and <code>authmethod</code> is set to <code>rsa-signature</code>. <p>Enter the method for authenticating remote clients or peers when they connect to the FortiGate unit:</p> <ul style="list-style-type: none"> • Type <code>any</code> to accept any remote client or peer (peer IDs are not used for authentication purposes). The <code>mode</code> attribute can be set to <code>aggressive</code> or <code>main</code>. You can use this option with RSA Signature authentication. But, for highest security, you should configure a PKI user/group for the peer and set Peer Options to Accept this peer certificate only. • Type <code>one</code> to authenticate either a remote peer or client that has a dynamic IP address and connects using a unique identifier over a dedicated tunnel, or more than one dialup client that connects through the same tunnel using the same (shared) identifier. Use the <code>peerid</code> field to set the peer ID. If more than one dialup client will be connecting using the same (shared) identifier, set <code>mode</code> to <code>aggressive</code>. | any |

| Variable | Description | Default |
|--------------------------------------|---|--------------------------|
| | <ul style="list-style-type: none"> Type <code>dialup</code> to authenticate dialup VPN clients that use unique identifiers and preshared keys (or unique preshared keys only) to connect to the VPN through the same VPN tunnel. In this case, you must create a dialup user group for authentication purposes. Use the <code>usrgrp</code> field to set the user group name. If the dialup clients use unique identifiers and preshared keys, set <code>mode</code> to <code>aggressive</code>. If the dialup clients use preshared keys only, set <code>mode</code> to <code>main</code>. Type <code>peer</code> to authenticate one (or more) certificate holders based on a particular (or shared) certificate. Use the <code>peer</code> field to enter the certificate name. Set <code>mode</code> to <code>aggressive</code> if the remote peer or client has a dynamic IP address. Type <code>peergrp</code> to authenticate certificate holders that use unique certificates. In this case, you must create a group of certificate holders for authentication purposes. Use the <code>peergrp</code> field to set the certificate group name. The <code>mode</code> attribute can be set to <code>aggressive</code> or <code>main</code>. Set <code>mode</code> to <code>aggressive</code> if the remote peer or client has a dynamic IP address. | |
| priority <prio> | <p>This value is used to break ties in selection of dialup routes. In the case that both routes have the same priority, the egress index for the routes will be used to determine the selected route.</p> <p>Set <prio> to a value between 0 and 4 294 967 295.</p> | 0 |
| proposal <encryption_combination> | <p>Select a minimum of one and a maximum of three encryption-message digest combinations for the phase 1 proposal (for example, <code>3des-md5</code>). The remote peer must be configured to use at least one of the proposals that you define. Use a space to separate the combinations.</p> <p>You can choose any of the following abbreviated symmetric key encryption algorithms:</p> <ul style="list-style-type: none"> <code>des</code> — Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. <code>3des</code> — Triple-DES, in which plain text is encrypted three times by three keys. <code>aes128</code> — A 128-bit block algorithm that uses a 128-bit key. <code>aes192</code> — A 128-bit block algorithm that uses a 192-bit key. <code>aes256</code> — A 128-bit block algorithm that uses a 256-bit key. | aes128-sha1 3des-sha1 |

| Variable | Description | Default |
|---|---|-------------------------------|
| | <ul style="list-style-type: none"> <code>aria128</code> — A 128-bit Korean block algorithm that uses a 128-bit key. <code>aria192</code> — A 128-bit Korean block algorithm that uses a 192-bit key. <code>aria256</code> — A 128-bit Korean block algorithm that uses a 256-bit key. <code>seed</code> — A 128-bit Korean block algorithm that uses a 128-bit key. <p>The ARIA and seed algorithms are not available on some models.</p> <p>You can select any of the following message digests to check the authenticity of messages during an encrypted session:</p> <ul style="list-style-type: none"> <code>md5</code> — Message Digest 5, the hash algorithm developed by RSA Data Security. <code>sha1</code> — Secure Hash Algorithm 1, which produces a 160-bit message digest. <code>sha256</code> — Secure Hash Algorithm 2, which produces a 256-bit message digest. <code>sha384</code> — Secure Hash Algorithm 2, which produces a 384-bit message digest. <code>sha512</code> — Secure Hash Algorithm 2, which produces a 512-bit message digest. | |
| <code>psksecret <preshared_key></code> | <p>This field is available when <code>authmethod</code> is set to <code>psk</code>.</p> <p>Enter the pre-shared key. The pre-shared key must be the same on the remote VPN gateway or client and should only be known by network administrators. The key must consist of at least 6 printable characters. For optimum protection against currently known attacks, the key should consist of a minimum of 16 randomly chosen alphanumeric characters.</p> | <p>*</p> <p>(No default.)</p> |
| <code>remote-gw <address_ipv4></code> | <p>This field is available when <code>type</code> is set to <code>static</code>.</p> <p>Enter the static IP address of the remote VPN peer.</p> | 0.0.0.0 |
| <code>remotegw-ddns <domain_name></code> | <p>This field is available when <code>type</code> is set to <code>ddns</code>.</p> <p>Enter the identifier of the remote peer (for example, a fully qualified domain name).</p> <p>Use this setting when the remote peer has a static domain name and a dynamic IP address (the IP address is obtained dynamically from an ISP and the remote peer subscribes to a dynamic DNS service).</p> | Null. |
| <code>rsa-certificate <server_certificate></code> | <p>This field is available when <code>authmethod</code> is set to <code>rsa-signature</code>.</p> <p>Enter the name of the signed personal certificate for the FortiGate unit. You must install the server certificate before you enter the server certificate name. For more information, see “vpn certificate local” on page 1006.</p> | Null. |

| Variable | Description | Default |
|---|--|---------------|
| type <remote_gw_type> | <p>Enter the connection type of the remote gateway:</p> <ul style="list-style-type: none"> If the remote VPN peer has a static IP address, type <code>static</code>. Use the <code>remotegw</code> field to enter the IP address. If the remote VPN peer has a dynamically assigned IP address (DHCP or PPPoE), type <code>dynamic</code>. If the remote VPN peer has a dynamically assigned IP address and subscribes to a dynamic DNS service, type <code>ddns</code>. Use the <code>remotegw-ddns</code> field to enter the domain name of the remote VPN peer. | static |
| usrgrp <group_name> | <p>This field is available when <code>type</code> is set to <code>dynamic</code>, <code>authmethod</code> is set to <code>psk</code>, and <code>peertype</code> is set to <code>dialup</code>.</p> <p>Enter the name of the group of dialup VPN clients to authenticate. The user group must be added to the FortiGate configuration before it can be cross-referenced here. For more information, see “user group” on page 722, “user ldap” on page 726, “user local” on page 729, and “user radius” on page 735.</p> | Null. |
| xauthtype <XAuth_type> | <p>Optionally configure XAuth (eXtended Authentication):</p> <ul style="list-style-type: none"> Type <code>disable</code> to disable XAuth. Type <code>client</code> to configure the FortiGate unit to act as an XAuth client. Use the <code>authuser</code> field to add the XAuth user name and password. Type <code>auto</code>, <code>pap</code>, or <code>chap</code> to configure the FortiGate unit as an XAuth server. These options are available only when <code>type</code> is <code>dynamic</code>. Use the <code>authusrgrp</code> field to specify the user group containing members that will be authenticated using XAuth. | disable |
| xauthexpire {on-disconnect on-rekey} | <p>Choose when the authentication with XAUTH expires:</p> <ul style="list-style-type: none"> <code>on-disconnect</code> — when the tunnel closes <code>on-rekey</code> — when the phase 1 encryption key expires | on-disconnect |

ipsec phase1-interface

Use this command to define a phase 1 definition for a route-based (interface mode) IPsec VPN tunnel that generates authentication and encryption keys automatically. A new interface of type “tunnel” with the same name is created automatically as the local end of the tunnel.

Optionally, you can create a route-based phase 1 definition to act as a backup for another IPsec interface. See the [monitor <phase1>](#) field.

To complete the configuration of an IPsec tunnel, you need to:

- configure phase 2 settings (see “[ipsec phase2-interface](#)” on page 803)
- configure a firewall policy to pass traffic from the local private network to the tunnel interface
- configure a static route via the IPsec interface to the private network at the remote end of the tunnel
- optionally, define the IP addresses for each end of the tunnel to enable dynamic routing through the tunnel or to enable pinging of each end of the tunnel for testing

Syntax

```
config vpn ipsec phase1-interface
edit <gateway_name>
    set add-gw-route {enable | disable}
    set add-route {enable | disable}
    set assign-ip {enable | disable}
    set assign-ip-from {range | usrgroup}
    set assign-ip-type {ip | subnet}
    set authmethod <authentication_method>
    set authpasswd <password>
    set authusr <user_name>
    set authusrgroup <group_name>
    set auto-negotiate {enable | disable}
    set banner <string>
    set client-auto-negotiate {enable | disable}
    set client-keep-alive {enable | disable}
    set default-gw <gw_ip>
    set default-gw-priority <int>
    set dhgroup {1 2 5 14}
    set distance <int>
    set dns-mode {auto | manual}
    set domain <string>
    set dpd {enable | disable}
    set dpd-retrycount <retry_integer>
    set dpd-retryinterval <seconds> [<milliseconds>]
    set forticlient-enforcement {enable | disable}
    set fragmentation {enable | disable}
    set ike-version {1 | 2}
    set include-local-lan {enable | disable}
    set interface <interface_name>
    set ip-version <4 | 6>
    set ipv4-dns-server1
    set ipv6-dns-server1
```

```
set ipv4-dns-server2
set ipv6-dns-server2
set ipv4-dns-server3
set ipv6-dns-server3
set ipv4-end-ip <ip4addr>
set ipv6-end-ip <ip6addr>
set ipv4-netmask <ip4mask>
set ipv4-split-include <address_name>
set ipv4-start-ip <ip4addr>
set ipv6-start-ip <ip6addr>
set ipv4-wins-server1
set ipv4-wins-server2
set ipv6-prefix <ip6prefix>
set keepalive <seconds>
set keylife <seconds>
set local-gw <address_ipv4>
set local-gw6 <address_ipv6>
set localid <local_id>
set localid-type {auto | fqdn | user-fqdn | keyid
| address | asn1dn}
set mode {aggressive | main}
set mode-cfg {enable | disable}
set mode-cfg-ip-version {4|6}
set monitor <phase1>
set monitor-hold-down-delay <seconds_int>
set nattraversal {enable | disable}
set negotiate-timeout <seconds_int>
set npu-offload {enable | disable}
set peer <CA_certificate_name>
set peerid <peer_id>
set peergrp <certificate_group_name>
set peertype <authentication_method>
set priority <prio>
set proposal <encryption_combination>
set psksecret <preshared_key>
set remote-gw <address_ipv4>
set remote-gw6 <address_ipv6>
set remotegw-ddns <domain_name>
set rsa-certificate <server_certificate>
set save-password {enable | disable}
set send-cert-chain {enable | disable}
set split-include-service <service_group_name>
set type <remote_gw_type>
set unity-support {enable | disable}
set usrgrp <group_name>
set xauthtype <XAuth_type>
set xauthexpire {on-disconnect | on-rekey}
```

```

config ipv4-exclude-range
    edit <entry_id>
        set start-ip <ipaddr>
        set end-ip <ipaddr>
    end
config ipv6-exclude-range
    edit <entry_id>
        set start-ip <ipaddr>
        set end-ip <ipaddr>
    end
end

```



You must specify values for `proposal` and `interface`. A `remote-gw` value may be required depending on the value of the `type` attribute. You must also enter a preshared key or a certificate name depending on the value of `authmethod`. All other fields are optional.

| Variable | Description | Default |
|------------------------------------|---|-------------|
| edit <gateway_name> | Enter a name (maximum 15 characters) for the remote gateway. If <code>type</code> is <code>dynamic</code> , the maximum name length is further reduced depending on the number of dialup tunnels that can be established: by 2 for up to 9 tunnels, by 3 for up to 99 tunnels, 4 for up to 999 tunnels, and so on | No default. |
| add-gw-route {enable disable} | Enable to automatically add a route to the remote gateway specified in <code>remote-gw</code> . Note: This command is deprecated. Use the <code>dynamic-gateway {enable disable}</code> field in <code>config router static</code> instead. | disable |
| add-route {enable disable} | Enable to add a route to the client's peer destination selector. Disable if you use dynamic routing over the tunnel. This is available only when <code>mode-cfg</code> is enabled. | enable |
| assign-ip {enable disable} | For a client, enable to request an IP address from the server. For a server, enable to assign an IP address to a dialup client. This is available if <code>mode-cfg</code> (IKE Configuration Method) is enabled. | enable |

| Variable | Description | Default |
|------------------------------------|--|-------------|
| assign-ip-from {range usrgrp} | <p>Select source of IP address assigned to an IKE Configuration Method client.</p> <p>range — Assign an IP address from the range defined in <code>ipv4-start-ip</code> and <code>ipv4-end-ip</code> (<code>ipv6-start-ip</code> and <code>ipv4-end-ip</code> for IPv6 clients).</p> <p>usrgrp — Assign the address defined in the RADIUS Framed-IP-Address for the user. This is available when the VPN is configured to authenticate clients with XAuth. <code>xauthtype</code> must be <code>auto</code>, <code>pap</code>, or <code>chap</code>. This is available only if <code>ike-version</code> is 1.</p> <p>This is available if <code>mode-cfg</code> (IKE Configuration Method) is enabled.</p> | range |
| assign-ip-type {ip subnet} | <p>Select the type of IP address assigned to an IKE Configuration Method client:</p> <p>ip — assign a single IP address to the client, as configured in <code>assign-ip-from</code>.</p> <p>subnet — assign an IP address to each end of the VPN tunnel, as configured in <code>assign-ip-from</code>. This type of IP address assignment facilitates the use of dynamic routing through the tunnel.</p> <p>This is available if <code>mode-cfg</code> (IKE Configuration Method) is enabled.</p> | ip |
| authmethod <authentication_method> | <p>Specify the authentication method:</p> <ul style="list-style-type: none"> Enter <code>psk</code> to authenticate using a pre-shared key. Use <code>psksecret</code> to enter the pre-shared key. Enter <code>rsa-signature</code> to authenticate using a digital certificate. Use <code>set rsa-certificate</code> to enter the name of the digital certificate. <p>You must configure certificates before selecting <code>rsa-signature</code> here. For more information, see “execute vpn certificate local” on page 1006 and “vpn certificate ca” on page 757.</p> | psk |
| authpasswd <password> | <p>This field is available when <code>xauthtype</code> is set to <code>client</code>.</p> <p>Enter the XAuth client password for the FortiGate unit.</p> | No default. |
| authusr <user_name> | <p>This field is available when <code>xauthtype</code> is set to <code>client</code>.</p> <p>Enter the XAuth client user name for the FortiGate unit.</p> | Null |

| Variable | Description | Default |
|---|--|---------|
| authusrgrp <group_name> | <p>This field is available when <code>xauthtype</code> is set to <code>auto</code>, <code>pap</code>, or <code>chap</code>.</p> <p>When the FortiGate unit is configured as an XAuth server, enter the user group to authenticate remote VPN peers. The user group can contain local users, LDAP servers, and RADIUS servers. The user group must be added to the FortiGate configuration before the group name can be cross-referenced. For more information, see “user group” on page 722, “user ldap” on page 726, “user local” on page 729, and “user radius” on page 735.</p> | Null |
| auto-negotiate {enable disable} | Enable to keep trying to negotiate an IKE SA even if the link is down. The primary use of this feature is in cases where there are multiple redundant tunnels and you prefer the primary connection if it can be established. | enable |
| banner <string> | Specify a message to send to IKE Configuration Method clients. Some clients display this message to users. This is available if <code>mode-cfg</code> (IKE Configuration Method) is enabled. | Null |
| client-auto-negotiate {enable disable} | Enable or disable allowing the client to bring up the tunnel when there is no traffic. This is available when <code>type</code> is <code>dynamic</code> and <code>mode-cfg</code> is enabled. | disable |
| client-keep-alive {enable disable} | Enable or disable allowing the client to keep the tunnel up when there is no traffic. This is available when <code>type</code> is <code>dynamic</code> and <code>mode-cfg</code> is enabled. | disable |
| default-gw <gw_ip> | <p>If the IPSec interface has a different default route than other traffic, enter the next hop router IP address. Be sure to set <code>default-gw-priority</code> to a higher priority (lower value) than the general default route.</p> <p>This is available when <code>type</code> is <code>dynamic</code>. The route it creates is not visible in the routing table.</p> | 0.0.0.0 |
| default-gw-priority <int> | If you set <code>default-gw</code> , set the priority to a lower value (higher priority) than the general default route. | 0 |
| dhgrp {1 2 5 14} | Type 1, 2, 5, and/or 14 to select one or more Diffie-Hellman groups from DH group 1, 2, 5, and 14 respectively. At least one of the DH group settings on the remote peer or client must be identical to one of the selections on the FortiGate unit. | 5 |
| distance <int> | Configure the administrative distance for routes added when a dialup IPSec connection is established. Using administrative distance you can specify the relative priorities of different routes to the same destination. A lower administrative distance indicates a more preferred route. Distance can be an integer from 1-255. See also router static “distance <distance>” on page 447 . | 1 |

| Variable | Description | Default |
|---|--|---------|
| dns-mode {auto manual} | Set DNS behavior when mode-cfg is enabled. auto — assign DNS servers in the following order: 1 servers assigned to interface by DHCP 2 per-VDOM assigned DNS servers 3 global DNS server manual — use DNS servers specified in <code>ipv4-dns-server1</code> , <code>ipv4-dns-server2</code> , etc. | manual |
| domain <string> | Specify a domain name to send to IKE Configuration Method clients. This is available if <code>mode-cfg</code> (IKE Configuration Method) is enabled. | Null |
| dpd {enable disable} | Enable or disable DPD (Dead Peer Detection). DPD detects the status of the connection between VPN peers. Enabling DPD facilitates cleaning up dead connections and establishing new VPN tunnels. DPD is not supported by all vendors and is not used unless DPD is supported and enabled by both VPN peers. | enable |
| dpd-retrycount <retry_integer> | This field is available when <code>dpd</code> is set to <code>enable</code> . The DPD retry count when <code>dpd</code> is set to <code>enable</code> . Set the number of times that the local VPN peer sends a DPD probe before it considers the link to be dead and tears down the security association (SA). The <code>dpd-retrycount</code> range is 0 to 10. To avoid false negatives due to congestion or other transient failures, set the retry count to a sufficiently high value for your network. | 3 |
| dpd-retryinterval <seconds> [<milliseconds>] | This field is available when <code>dpd</code> is set to <code>enable</code> . The DPD (Dead Peer Detection) retry interval is the time that the local VPN peer waits between sending DPD probes. Set the time in seconds plus, optionally, milliseconds. For example, for 2.5 seconds enter 2 500. The range is 1 to 60 seconds, 0 to 999 milliseconds. When the tunnel is starting, or if it has failed, a retry interval of 5 seconds is used if <code>dpd-retryinterval</code> is less than 5 seconds. | 5 |
| forticlient-enforcement {enable disable} | Enable to allow only FortiClient users to connect. | disable |
| fragmentation {enable disable} | Enable intra-IKE fragmentation support on re-transmission of fragmented packets. | enable |
| ike-version {1 2} | Select whether to use IKEv1 or IKEv2 (RFC 4306). | 1 |
| include-local-lan {enable disable} | Allow Unity clients to access their local LAN even if they are using split tunneling. This is available when <code>type</code> is <code>dynamic</code> and <code>mode-config</code> is enabled. | disable |

| Variable | Description | Default |
|--|--|---------------|
| interface <interface_name> | Enter the name of the physical, aggregate, or VLAN interface to which the IPsec tunnel will be bound. The FortiGate unit obtains the IP address of the interface from system interface settings (see “interface” on page 555) unless you specify a different IP address using the <code>local-gw <address_ipv4></code> attribute. | Null |
| ip-version <4 6> | Enter 4 for IPv4 encapsulation or 6 for IPv6 encapsulation. | 4 |
| ipv4-dns-server1 ipv6-dns-server1 ipv4-dns-server2 ipv6-dns-server2 ipv4-dns-server3 ipv6-dns-server3 | Enter DNS server addresses to provide to IKE Configuration Method clients. If the value is 0.0.0.0, no DNS server address is provided. Either the IPv4 or IPv6 version of these fields is available, depending on <code>mode-cfg-ip-version</code> . | 0.0.0.0 :: |
| ipv4-end-ip <ip4addr> ipv6-end-ip <ip6addr> | Set end of IP address range to assign to IKE Configuration Method clients. This is available when <code>mode-cfg</code> is enabled, <code>type</code> is <code>dynamic</code> , and <code>assign-ip-from</code> is <code>range</code> . Either the IPv4 or IPv6 version of this field is available, depending on <code>mode-cfg-ip-version</code> . | No default. |
| ipv4-netmask <ip4mask> | Set the netmask value to pass to IKE Configuration Method clients. | No default. |
| ipv4-split-include <address_name> | Select the address or address group that the client can reach through the VPN. This information is sent to the client as part of IKE Configuration Method. This is available only if <code>mode-cfg</code> is set to <code>enable</code> . | Null. |
| ipv4-start-ip <ip4addr> ipv6-start-ip <ip6addr> | Set start of IP address range to assign to IKE Configuration Method clients. This is available when <code>mode-cfg</code> is enabled, <code>type</code> is <code>dynamic</code> , and <code>assign-ip-from</code> is <code>range</code> . Either the IPv4 or IPv6 version of this field is available, depending on <code>mode-cfg-ip-version</code> . | No default. |
| ipv4-wins-server1 ipv4-wins-server2 | Enter WINS server addresses to provide to IKE Configuration Method clients. If the value is 0.0.0.0, no WINS server address is provided. | 0.0.0.0 |
| ipv6-prefix <ip6prefix> | Specify the size, in bits, of the network portion of the subnet address for IPv6 IKE Configuration Method clients. Range is 0 to 128. This is available when <code>mode-cfg-ip-version</code> is 6 and <code>assign-ip-type</code> is <code>subnet</code> . | 0 |

| Variable | Description | Default |
|---|--|---------------------------------|
| keepalive <seconds> | <p>This field is available when <code>nattraversal</code> is set to <code>enable</code>.</p> <p>Set the NAT traversal keepalive frequency. This number specifies (in seconds) how frequently empty UDP packets are sent through the NAT device to make sure that the NAT mapping does not change until P1 and P2 security associations expire. The keepalive frequency can be from 0 to 900 seconds.</p> | 5 |
| keylife <seconds> | <p>Set the keylife time. The keylife is the amount of time (in seconds) before the phase 1 encryption key expires. When the key expires, a new key is generated without interrupting service. The range is 120 to 172,800 seconds.</p> | 28800 |
| local-gw <address_ipv4> local-gw6 <address_ipv6> | <p>Optionally, specify a secondary IP address of the interface selected in <code>interface</code> to use for the local end of the VPN tunnel. <code>local-gw6</code> is available when <code>ip-version</code> is 6. <code>local-gw</code> is available when <code>ip-version</code> is 4.</p> <p>If you do not specify an IP address here, the FortiGate unit obtains the IP address of the interface from system interface settings (see “interface” on page 555).</p> | 0.0.0.0 for IPv4 :: for IPv6 |
| localid <local_id> | <p>Enter a local ID if the FortiGate unit is functioning as a VPN client and will use the local ID for authentication purposes.</p> <p>If you want to dedicate a tunnel to a FortiGate dialup client, you must assign a unique identifier (local ID) to the FortiGate client.</p> <p>Whenever you configure a unique identifier (local ID) on a FortiGate dialup client, you must enable aggressive mode on the FortiGate dialup server and also specify the identifier as a peer ID on the FortiGate dialup server.</p> | Null |
| localid-type {auto fqdn user-fqdn keyid address asn1dn} | <p>Select the type of <code>localid</code>:</p> <p><code>auto</code> — select type automatically</p> <p><code>fqdn</code> — Fully Qualified Domain Name</p> <p><code>user-fqdn</code> — Use User Fully Qualified Domain Name</p> <p><code>keyid</code> — Use Key Identifier ID</p> <p><code>address</code> — Use IP address ID</p> <p><code>asn1dn</code> — Use ASN.1 Distinguished Name ID</p> | auto |

| Variable | Description | Default |
|---------------------------------------|---|---------|
| mode {aggressive main} | <p>Enter <code>aggressive</code> or <code>main</code> (ID Protection) mode. Both modes establish a secure channel.</p> <p>In main mode, identifying information is hidden. Main mode is typically used when both VPN peers have static IP addresses.</p> <p>In aggressive mode, identifying information is exchanged in the clear. Aggressive mode is typically used when a remote peer or dialup client has a dynamic IP address. You must enable aggressive mode when the remote FortiGate unit has a dynamic IP address, or the remote VPN peer or client will be authenticated using an identifier (local ID).</p> <p>This is available if <code>ike-version</code> is 1.</p> | main |
| mode-cfg {enable disable} | <p>Enable IKE Configuration Method so that compatible clients can configure themselves with settings that the FortiGate unit provides.</p> <p>This is available if <code>type</code> is <code>dynamic</code>.</p> | disable |
| mode-cfg-ip-version {4 6} | Select whether an IKE Configuration Method client receives an IPv4 or IPv6 IP address. This is available if <code>mode-cfg</code> and <code>assign-ip</code> are enabled. | 4 |
| monitor <phase1> | <p>Optionally, this IPSec interface can act as a backup for another (primary) IPSec interface. Enter the name of the primary interface.</p> <p>The backup interface is used only while the primary interface is out of service. <code>dpd</code> must be enabled.</p> <p>A primary interface can have only one backup interface and cannot act as a backup for another interface.</p> | Null. |
| monitor-hold-down-delay <seconds_int> | Enter the number of seconds to delay returning traffic to the primary interface from backup after the primary interface becomes stable again. Range: 0 to 31 536 000 seconds. | 0 |
| natraversal {enable disable} | Enable NAT traversal if you expect the IPSec VPN traffic to go through a gateway that performs NAT. If no NAT device is detected, enabling NAT traversal has no effect. Both ends of the VPN must have the same NAT traversal setting. If you enable NAT traversal you can set the <code>keepalive</code> frequency. | enable |
| negotiate-timeout <seconds_int> | Enter how long in seconds the FortiGate unit will wait for the IKE SA to be negotiated. Range: 1 to 300 seconds. | 30 |
| npu-offload {enable disable} | Enable or disable offload of VPN session to NPU. | enable |

| Variable | Description | Default |
|-------------------------------------|---|---------|
| peer <CA_certificate_name> | <p>This field is available when <code>authmethod</code> is set to <code>rsa-signature</code> and <code>peertype</code> is set to <code>peer</code>.</p> <p>Enter the name of the peer (CA) certificate that will be used to authenticate remote VPN clients or peers. Use the command <code>config user peer</code> to add peer certificates. Peer certificates must be added to the FortiGate configuration before they can be cross-referenced. For more information, see “user peer” on page 732.</p> | Null |
| peerid <peer_id> | <p>This field is available when <code>peertype</code> is set to <code>one</code>.</p> <p>Enter the peer ID that will be used to authenticate remote clients or peers by peer ID.</p> | Null |
| peergrp <certificate_group_name> | <p>This field is available when <code>type</code> is set to <code>dynamic</code>, <code>authmethod</code> is set to <code>rsa-signature</code>, and <code>peertype</code> is set to <code>peergrp</code>.</p> <p>Enter the name of the peer certificate group that will be used to authenticate remote clients or peers. You must create the peer certificate group before the group name can be cross-referenced. For more information, see “user peergrp” on page 734.</p> | Null |
| peertype <authentication_method> | <p>The following attributes are available under the following conditions:</p> <ul style="list-style-type: none"> <code>dialup</code> is available when <code>type</code> is set to <code>dynamic</code> and <code>authmethod</code> is set to <code>psk</code>. <code>peer</code> is available when <code>authmethod</code> is set to <code>rsa-signature</code>. <code>peergrp</code> is available when <code>type</code> is set to <code>dynamic</code> and <code>authmethod</code> is set to <code>rsa-signature</code>. <p>Enter the method for authenticating remote clients or peers when they connect to the FortiGate unit:</p> <ul style="list-style-type: none"> Type <code>any</code> to accept any remote client or peer (peer IDs are not used for authentication purposes). The <code>mode</code> attribute can be set to <code>aggressive</code> or <code>main</code>. You can use this option with RSA Signature authentication. But, for highest security, you should configure a PKI user/group for the peer and set Peer Options to Accept this peer certificate only. | any |

| Variable | Description | Default |
|--------------------------------------|--|--------------------------|
| | <ul style="list-style-type: none"> Type <code>one</code> to authenticate either a remote peer or client that has a dynamic IP address and connects using a unique identifier over a dedicated tunnel, or more than one dialup client that connects through the same tunnel using the same (shared) identifier. Use the <code>peerid</code> field to set the peer ID. If more than one dialup client will be connecting using the same (shared) identifier, set <code>mode</code> to <code>aggressive</code>. Type <code>dialup</code> to authenticate dialup VPN clients that use unique identifiers and preshared keys (or unique preshared keys only) to connect to the VPN through the same VPN tunnel. In this case, you must create a dialup user group for authentication purposes. Use the <code>usrgrp</code> field to set the user group name. If the dialup clients use unique identifiers and preshared keys, set <code>mode</code> to <code>aggressive</code>. If the dialup clients use preshared keys only, set <code>mode</code> to <code>main</code>. Type <code>peer</code> to authenticate one (or more) certificate holders based on a particular (or shared) certificate. Use the <code>peer</code> field to enter the certificate name. Set <code>mode</code> to <code>aggressive</code> if the remote peer or client has a dynamic IP address. Type <code>peergrp</code> to authenticate certificate holders that use unique certificates. In this case, you must create a group of certificate holders for authentication purposes. Use the <code>peergrp</code> field to set the certificate group name. The <code>mode</code> attribute can be set to <code>aggressive</code> or <code>main</code>. Set <code>mode</code> to <code>aggressive</code> if the remote peer or client has a dynamic IP address. | |
| priority <prio> | <p>This value is used to be break ties in selection of dialup routes. In the case that both routes have the same priority, the egress index for the routes will be used to determine the selected route.</p> <p>Set <prio> to a value between 0 and 4 294 967 295.</p> | 0 |
| proposal <encryption_combination> | <p>Select a minimum of one and a maximum of three encryption-message digest combinations for the phase 1 proposal (for example, <code>3des-md5</code>). The remote peer must be configured to use at least one of the proposals that you define. Use a space to separate the combinations.</p> | aes128-sha1 3des-sha1 |

| Variable | Description | Default |
|---------------------------|--|-------------------------------|
| | <p>You can choose any of the following abbreviated symmetric key encryption algorithms:</p> <ul style="list-style-type: none"> • <code>des</code> — Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. • <code>3des</code> — Triple-DES, in which plain text is encrypted three times by three keys. • <code>aes128</code> — A 128-bit block algorithm that uses a 128-bit key. • <code>aes192</code> — A 128-bit block algorithm that uses a 192-bit key. • <code>aes256</code> — A 128-bit block algorithm that uses a 256-bit key. • <code>aria128</code> — A 128-bit Korean block algorithm that uses a 128-bit key. • <code>aria192</code> — A 128-bit Korean block algorithm that uses a 192-bit key. • <code>aria256</code> — A 128-bit Korean block algorithm that uses a 256-bit key. • <code>seed</code> — A 128-bit Korean block algorithm that uses a 128-bit key. <p>The ARIA and seed algorithms are not available on some models.</p> <p>You can select any of the following message digests to check the authenticity of messages during an encrypted session:</p> <ul style="list-style-type: none"> • <code>md5</code> — Message Digest 5, the hash algorithm developed by RSA Data Security. • <code>sha1</code> — Secure Hash Algorithm 1, which produces a 160-bit message digest. • <code>sha256</code> — Secure Hash Algorithm 2, which produces a 256-bit message digest. • <code>sha384</code> — Secure Hash Algorithm 2, which produces a 384-bit message digest. • <code>sha512</code> — Secure Hash Algorithm 2, which produces a 512-bit message digest. | |
| psksecret <preshared_key> | <p>This field is available when <code>authmethod</code> is set to <code>psk</code>.</p> <p>Enter the pre-shared key. The pre-shared key must be the same on the remote VPN gateway or client and should only be known by network administrators. The key must consist of at least 6 printable characters. For optimum protection against currently known attacks, the key should consist of a minimum of 16 randomly chosen alphanumeric characters.</p> | <p>*</p> <p>(No default.)</p> |

| Variable | Description | Default |
|---|---|--|
| remote-gw <address_ipv4> remote-gw6 <address_ipv6> | This field is available when type is set to static. Enter the static IP address of the remote VPN peer. remote-gw6 is available when ip-version is 6. remote-gw is available when ip-version is 4. | 0.0.0.0 for IPv4 :: for IPv6 |
| remotegw-ddns <domain_name> | This field is available when type is set to ddns and ip-version is set to 4. Enter the identifier of the remote peer (for example, a fully qualified domain name). Use this setting when the remote peer has a static domain name and a dynamic IP address (the IP address is obtained dynamically from an ISP and the remote peer subscribes to a dynamic DNS service). | Null |
| rsa-certificate <server_certificate> | This field is available when authmethod is set to rsa-signature. Enter the name of the signed personal certificate for the FortiGate unit. You must install the server certificate before you enter the server certificate name. For more information, see “vpn certificate local” on page 1006 . | Null |
| save-password {enable disable} | Enable or disable client saving Xauth user name and password. | disable |
| send-cert-chain {enable disable} | Enable or disable sending of the certificate chain, rather than a single certificate. | enable |
| split-include-service <service_group_name> | Select the service types that the client can reach through the VPN. This information is sent to the client as part of IKE Configuration Method when mode-cfg is enabled. | Null |
| type <remote_gw_type> | Enter the connection type of the remote gateway: <ul style="list-style-type: none">• If the remote VPN peer has a static IP address, type static. Use the remotegw field to enter the IP address.• If the remote VPN peer has a dynamically assigned IP address (DHCP or PPPoE), type dynamic.• If the remote VPN peer has a dynamically assigned IP address and subscribes to a dynamic DNS service, type ddns. Use the remotegw-ddns field to enter the domain name of the remote VPN peer. This option is not available if ip-version is 6. | static |
| unity-support {enable disable} | Enable support for Cisco Unity IKE Configuration Method extensions in either a server or a client. This is available for IKEv1 only. | enable |

| Variable | Description | Default |
|--|--|---------------|
| usrgrp <group_name> | <p>This field is available when <code>type</code> is set to <code>dynamic</code>, <code>authmethod</code> is set to <code>psk</code>, and <code>peertype</code> is set to <code>dialup</code>.</p> <p>Enter the name of the group of dialup VPN clients to authenticate. The user group must be added to the FortiGate configuration before it can be cross-referenced here. For more information, see “user group” on page 722, “user ldap” on page 726, “user local” on page 729, and “user radius” on page 735.</p> | Null |
| xauthtype <XAuth_type> | <p>Optionally configure XAuth (eXtended Authentication):</p> <ul style="list-style-type: none"> Type <code>disable</code> to disable XAuth. Type <code>client</code> to configure the FortiGate unit to act as an XAuth client. Use the <code>authuser</code> field to add the XAuth user name and password. Type <code>auto</code>, <code>pap</code>, or <code>chap</code> to configure the FortiGate unit as an XAuth server. These options are available only when <code>type</code> is <code>dynamic</code>. Use the <code>authusrgrp</code> field to specify the user group containing members that will be authenticated using XAuth. | disable |
| xauthexpire {on-disconnect on-rekey} | <p>Choose when the authentication with XAUTH expires:</p> <ul style="list-style-type: none"> <code>on-disconnect</code> — when the tunnel closes <code>on-rekey</code> — when the phase 1 encryption key expires | on-disconnect |
| config ipv4-exclude-range and config ipv6-exclude-range Variables This subcommand is available only when <code>mode-cfg</code> is enabled. | | |
| start-ip <ipaddr> | Enter the start of the exclude range. | No default. |
| end-ip <ipaddr> | Enter the end of the exclude range. | No default. |

ipsec phase2

Use this command to add or edit an IPSec tunnel-mode phase 2 configuration. The FortiGate unit uses the tunnel-mode phase 2 configuration to create and maintain an IPSec VPN tunnel with a remote VPN peer (the VPN gateway or client).

The phase 2 configuration consists of a name for the VPN tunnel, the name of an existing phase 1 configuration, the proposal settings (encryption and authentication algorithms) and DH group used for phase 2. For phase 2 to be successful, the FortiGate unit and the remote VPN peer must be configured with compatible proposal settings.

Syntax

```
config vpn ipsec phase2
  edit <tunnel_name>
    set add-route {enable | disable}
    set auto-negotiate {enable | disable}
    set dhcp-ipsec {enable | disable}
    set dhgrp {1 | 2 | 5 | 14}
    set dst-addr-type <type>
    set dst-end-ip <address_ipv4>
    set dst-name <address_name>
    set dst-port <dest_port_number>
    set dst-start-ip <address_ipv4>
    set dst-subnet <address_ipv4mask>
    set encapsulation {tunnel-mode | transport-mode}
    set keepalive {enable | disable}
    set keylife-type <keylife_type>
    set keylifekbs <kb_integer>
    set keylifeseconds <seconds>
    set l2tp {enable | disable}
    set pfs {enable | disable}
    set phase1name <gateway_name>
    set proposal <encrypt_digest>
    set protocol <protocol_integer>
    set replay {enable | disable}
    set route-overlap {overlap_option}
    set selector-match <match_type>
    set single-source {enable | disable}
    set src-addr-type <ip_source_name>
    set src-end-ip <address_ipv4>
    set src-name <address_name>
    set src-port <src_port_number>
    set src-start-ip <address_ipv4>
    set src-subnet <address_ipv4mask>
    set use-natip {enable | disable}
  end
```

The phase1name field is required. All other fields are optional.

| Variable | Description | Default |
|--------------------------------------|---|-------------|
| edit <tunnel_name> | Enter a name for the tunnel. | No default. |
| add-route {enable disable} | Enable only if you are running a dynamic routing protocol (RIP, OSPF, or BGP) and want the routes to be propagated to routing peers. | disable |
| auto-negotiate {enable disable} | Enable to negotiate the phase 2 security association (SA) automatically, even if there is no traffic. This repeats every five seconds until it succeeds. You can use this option on a dialup peer to ensure that the tunnel is available for peers at the server end to initiate traffic to the dialup peer. Otherwise, the tunnel does not exist until the dialup peer initiates traffic. | disable |
| dhcp-ipsec {enable disable} | This field is available when phase1name names a dialup gateway configuration. Enable dhcp-ipsec if the FortiGate unit acts as a dialup server and FortiGate DHCP relay will be used to assign VIP addresses to FortiClient dialup clients. The DHCP relay parameters must be configured separately. If you configure the DHCP server to assign IP addresses based on RADIUS user group attributes, you must also set the peertype to dialup and specify the usrgrp in vpn ipsec phase1 . For information about how to configure a DHCP server on a FortiGate interface, see “system dhcp server” on page 501 . For information about FortiGate DHCP relay, see “system interface” on page 555 . If the FortiGate unit acts as a dialup server and you manually assigned FortiClient dialup clients VIP addresses that match the network behind the dialup server, select Enable to cause the FortiGate unit to act as a proxy for the dialup clients. | disable |
| dhgrp {1 2 5 14} | Type 1, 2, 5, or 14 to select the Diffie-Hellman group to propose for Phase 2 of the IPSec VPN connection. Both VPN peers must use the same DH Group. | 5 |

| Variable | Description | Default |
|--|--|--------------------|
| dst-addr-type <type> | <p>Enter the type of destination address that corresponds to the recipient(s) or network behind the remote VPN peer or FortiGate dialup client:</p> <ul style="list-style-type: none"> To specify the IP address of a server or host, type <code>ip</code>. Enter the IP address using the <code>dst-start-ip</code> field. To specify a range of IP addresses, type <code>range</code>. Enter the starting and ending addresses using the <code>dst-start-ip</code>, and <code>dst-end-ip</code> fields. To specify a network address, type <code>subnet</code>. Enter the network address using the <code>dst-subnet</code> field. To specify a firewall address or address group, type <code>name</code>. Enter the address or address group name using the <code>dst-name</code> field. You must also select the <code>name</code> option for <code>src-addr-type</code>. You should not use this option if <code>ike-version</code> is 1. IKEv1 does not support the use of multiple addresses in selectors. Instead, use the default 0.0.0.0/0 subnet selector and rely on the firewall policy to limit destination addresses. | subnet |
| dst-end-ip <address_ipv4> | <p>This field is available when <code>dst-addr-type</code> is set to <code>range</code>. This field is not available if <code>phase1name</code> names a configuration that enables <code>mode-cfg</code>.</p> <p>Enter the highest destination IP address in the range of IP addresses.</p> | 0.0.0.0 |
| dst-name <address_name> | <p>This field is available when <code>dst-addr-type</code> is set to <code>name</code>. Enter the name of a firewall address or address group.</p> | No default. |
| dst-port <dest_port_number> | <p>Enter the port number that the remote VPN peer or FortiGate dialup client uses to transport traffic related to the specified service (see <code>protocol</code>). The range is 1 to 65535. To specify all ports, type 0.</p> | 0 |
| dst-start-ip <address_ipv4> | <p>This field is available when <code>dst-addr-type</code> is set to <code>range</code>.</p> <p>Enter the lowest destination IP address in the range of IP addresses.</p> | 0.0.0.0 |
| dst-subnet <address_ipv4mask> | <p>Enter the IP address and network mask that identifies the private network behind the remote VPN peer or FortiGate dialup client.</p> | 0.0.0.0 0.0.0.0 |
| encapsulation { tunnel-mode transport-mode } | <p>Select encapsulation:</p> <p>tunnel-mode — Encrypt both payload data and headers.</p> <p>transport-mode — Encrypt only the payload data. This is used when combining IPsec with another encapsulation, such as L2TP.</p> | tunnel-mode |
| keepalive { enable disable } | <p>Enable to automatically negotiate a new phase 2 security association (SA) before the current SA expires, keeping the tunnel up. Otherwise, a new SA is negotiated only if there is traffic.</p> | disable |

| Variable | Description | Default |
|--------------------------------|---|--------------------------|
| keylife-type <keylife_type> | <p>Set when the phase 2 key expires. When the key expires, a new key is generated without interrupting service.</p> <ul style="list-style-type: none"> To make the key expire after a period of time has expired and after an amount of data is transmitted, type <code>both</code>. To make the key expire after an amount of data is transmitted, type <code>kbs</code>. Use the <code>keylifekbs</code> field to set the amount of data that is transmitted. To make the key expire after a number of seconds elapses, type <code>seconds</code>. Use the <code>keylifeseconds</code> field to set the amount of time that elapses. | seconds |
| keylifekbs <kb_integer> | <p>This field is available when <code>keylife-type</code> is set to <code>kbs</code> or <code>both</code>.</p> <p>Set the number of Kbits of data to transmit before the phase 2 key expires. The range is 5120 to 4 294 967 295 Kbits.</p> | 5120 |
| keylifeseconds <seconds> | <p>This field is available when <code>keylife-type</code> is set to <code>seconds</code> or <code>both</code>.</p> <p>Set the number of seconds to elapse before the phase 2 key expires. <code>seconds</code> can be 120 to 172800 seconds.</p> | 1800 |
| l2tp {enable disable} | Enable L2TP traffic through this VPN. This is available if <code>encapsulation</code> is <code>transport-mode</code> and the phase 1 type is <code>dynamic</code> . | disable |
| pfs {enable disable} | Optionally, enable or disable perfect forward secrecy (PFS). PFS ensures that each key created during Phase 2 is unrelated to keys created during Phase 1 or to other keys created during Phase 2. PFS may cause minor delays during key generation. | enable |
| phase1name <gateway_name> | Enter a phase 1 gateway configuration name. You must add the phase 1 gateway definition to the FortiGate configuration before it can be cross-referenced. | Null |
| proposal <encrypt_digest> | <p>Enter a minimum of one and a maximum of three encryption-message digest combinations (for example, <code>3des-md5</code>). The remote peer must be configured to use at least one of the proposals that you define. Use a space to separate the combinations.</p> <p>You can enter any encryption-message digest combination except <code>null-null</code>.</p> | aes128-sha1 3des-sha1 |

| Variable | Description | Default |
|--|--|---------|
| | <p>Here is an explanation of the abbreviated encryption algorithms:</p> <ul style="list-style-type: none"> • <code>null</code> — Do not use an encryption algorithm. • <code>des</code> — Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. • <code>3des</code> — Triple-DES, in which plain text is encrypted three times by three keys. • <code>aes128</code> — A 128-bit block algorithm that uses a 128-bit key. • <code>aes192</code> — A 128-bit block algorithm that uses a 192-bit key. • <code>aes256</code> — A 128-bit block algorithm that uses a 256-bit key. • <code>aria128</code> — A 128-bit Korean block algorithm that uses a 128-bit key. • <code>aria192</code> — A 128-bit Korean block algorithm that uses a 192-bit key. • <code>aria256</code> — A 128-bit Korean block algorithm that uses a 256-bit key. • <code>seed</code> — A 128-bit Korean block algorithm that uses a 128-bit key. <p>The ARIA and seed algorithms are not available on some models.</p> <p>You can enter any of the following message digests to check the authenticity of messages during an encrypted session:</p> <ul style="list-style-type: none"> • <code>null</code> — Do not use a message digest. • <code>md5</code> — Message Digest 5, the hash algorithm developed by RSA Data Security. • <code>sha1</code> — Secure Hash Algorithm 1, which produces a 160-bit message digest. • <code>sha256</code> — Secure Hash Algorithm 2, which produces a 256-bit message digest. | |
| <code>protocol</code> <code><protocol_integer></code> | <p>This field is available when <code>selector</code> is set to <code>specify</code>.</p> <p>Enter the IP protocol number for the service. The range is 1 to 255. To specify all services, type 0.</p> | 0 |
| <code>replay</code> <code>{enable disable}</code> | <p>Optionally, enable or disable replay detection. Replay attacks occur when an unauthorized party intercepts a series of IPSec packets and replays them back into the tunnel. Enable replay detection to check the sequence number of every IPSec packet to see if it has been received before. If packets arrive out of sequence, the FortiGate units discards them.</p> <p>You can configure the FortiGate unit to send an alert email when it detects a replay packet. See “alertemail” on page 55.</p> | enable |

| Variable | Description | Default |
|-------------------------------------|--|---------|
| route-overlap {overlap_option} | Specify how FortiGate unit handles multiple dialup users with the same IP source address. Set <code>overlap_option</code> to one of the following: allow — allow overlapping routes use-new — delete the old route and add the new route use-old — use the old route and do not add the new route | use-new |
| selector-match <match_type> | The peer's IPSec selectors are compared to FortiGate phase 2 selectors, which are any of <code>src-start-ip</code> / <code>src-end-ip</code> , <code>src-subnet</code> , <code>dst-subnet</code> , <code>dst-start-ip</code> / <code>dst-end-ip</code> . The <code>match_type</code> value can be one of: exact — peer's selector must match exactly subset — peer's selector can be a subset of this selector auto — use exact or subset match as needed (default) Note: This field is configured automatically when upgrading a FortiOS version 2.80 VPN to version 3.0. You should not set this field when configuring a new VPN. This field does not apply to IKEv2 connections. | auto |
| single-source {enable disable} | Enable if <code>src-addr-type</code> is name and hosts on the internal network will initiate communication sessions with remote dialup clients. | disable |
| src-addr-type <ip_source_name> | If the FortiGate unit is a dialup server, enter the type of source address that corresponds to the local sender(s) or network behind the FortiGate dialup server: <ul style="list-style-type: none">To specify the IP address of a server or host, type <code>ip</code>. Enter the IP address using the <code>src-start-ip</code> field.To specify a range of IP addresses, type <code>range</code>. Enter the starting and ending addresses using the <code>src-start-ip</code> and <code>src-end-ip</code> fields.To specify a network address, type <code>subnet</code>. Enter the network address using the <code>src-subnet</code> field.To specify a firewall address or address group, type <code>name</code>. Enter the address or address group name using the <code>src-name</code> field. You must also select the name option for <code>dst-addr-type</code>. You should not use this option if <code>ike-version</code> is 1. IKEv1 does not support the use of multiple addresses in selectors. Instead, use the default 0.0.0.0/0 subnet selector and rely on the firewall policy to limit source addresses. If the FortiGate unit is a dialup client, <code>src-addr-type</code> must refer to the server(s), host(s), or private network behind the FortiGate dialup client. | subnet |
| src-end-ip <address_ipv4> | This field is available when <code>src-addr-type</code> is set to <code>range</code> . Enter the highest source IP address in the range of IP addresses. | 0.0.0.0 |

| Variable | Description | Default |
|----------------------------------|---|--------------------|
| src-name <address_name> | This field is available when <code>src-addr-type</code> is set to <code>name</code> . Enter the name of a firewall address or address group. | No default. |
| src-port <src_port_number> | If the FortiGate unit is a dialup server, enter the port number that the FortiGate dialup server uses to transport traffic related to the specified service (see <code>protocol</code>). If the FortiGate unit is a dialup client, enter the port number that the FortiGate dialup client uses to transport traffic related to the specified service. The <code>src-port</code> range is 1 to 65535. To specify all ports, type 0. | 0 |
| src-start-ip <address_ipv4> | This field is available when <code>src-addr-type</code> is set to <code>range</code> . Enter the lowest source IP address in the range of IP addresses. | 0.0.0.0 |
| src-subnet <address_ipv4mask> | If the FortiGate unit is a dialup server, enter the IP address and network mask that identifies the private network behind the FortiGate dialup server. If the FortiGate unit is a dialup client, enter the IP address and network mask that identifies the private network behind the FortiGate dialup client. | 0.0.0.0 0.0.0.0 |
| use-natip {enable disable} | By default, when outbound NAT is used, the FortiGate unit public interface IP address is the source selector. If you disable <code>use-natip</code> , the source selector is as specified in <code>src-start-ip</code> / <code>src-end-ip</code> or <code>src-subnet</code> . Note: This field is configured automatically when upgrading a FortiOS version 2.80 VPN to version 3.0. You should not set this field when configuring a new VPN. | enable |

ipsec phase2-interface

Use this command to add a phase 2 configuration for a route-based (interface mode) IPSec tunnel or edit an existing interface-mode phase 2 configuration. This command is available only in NAT/Route mode.

Syntax

```
config vpn ipsec phase2-interface
edit <tunnel_name>
    set auto-negotiate {enable | disable}
    set dhcp-ipsec {enable | disable}
    set dhgrp {1 | 2 | 5 | 14}
    set dst-addr-type <type>
    set dst-end-ip <address_ipv4>
    set dst-end-ip6 <address_ipv6>
    set dst-name <address_name>
    set dst-port <dest_port_number>
    set dst-start-ip <address_ipv4>
    set dst-start-ip6 <address_ipv6>
    set dst-subnet <address_ipv4mask>
    set dst-subnet6 <address_ipv6mask>
    set encapsulation {tunnel-mode | transport-mode}
    set keepalive {enable | disable}
    set keylife-type <keylife_type>
    set keylifekbs <kb_integer>
    set keylifeseconds <seconds>
    set l2tp {enable | disable}
    set pfs {enable | disable}
    set phaselname <gateway_name>
    set proposal <encrypt_digest>
    set protocol <protocol_integer>
    set replay {disable | enable}
    set route-overlap {overlap_option}
    set single-source {disable | enable}
    set src-addr-type <ip_source_name>
    set src-end-ip <address_ipv4>
    set src-end-ip6 <address_ipv6>
    set src-name <address_name>
    set src-port <src_port_number>
    set src-start-ip <address_ipv4>
    set src-start-ip6 <address_ipv6>
    set src-subnet <address_ipv4mask>
    set src-subnet6 <address_ipv6mask>
end
```

The phase1name field is required. All other fields are optional.

| Variable | Description | Default |
|--|---|-------------|
| edit < tunnel_name > | Enter a name for the phase 2 tunnel configuration. | No default. |
| auto-negotiate { enable disable } | <p>Enable to negotiate the phase 2 security association (SA) automatically, even if there is no traffic. This repeats every five seconds until it succeeds.</p> <p>You can use this option on a dialup peer to ensure that the tunnel is available for peers at the server end to initiate traffic to the dialup peer. Otherwise, the tunnel does not exist until the dialup peer initiates traffic.</p> | disable |
| dhcp-ipsec { enable disable } | <p>This field is available when phase1name names a dialup gateway configuration.</p> <p>This field is not available if phase1name names a configuration that enables mode-cfg.</p> <p>Enable dhcp-ipsec if the FortiGate unit acts as a dialup server and FortiGate DHCP relay will be used to assign VIP addresses to FortiClient dialup clients. The DHCP relay parameters must be configured separately.</p> <p>If you configure the DHCP server to assign IP addresses based on RADIUS user group attributes, you must also set the peertype to dialup and specify the usrgrp in vpn ipsec phase1.</p> <p>For information about how to configure a DHCP server on a FortiGate interface, see “system dhcp server” on page 501. For information about FortiGate DHCP relay, see “system interface” on page 555.</p> <p>If the FortiGate unit acts as a dialup server and you manually assigned FortiClient dialup clients VIP addresses that match the network behind the dialup server, select Enable to cause the FortiGate unit to act as a proxy for the dialup clients.</p> | disable |
| dhgrp { 1 2 5 14 } | Type 1, 2, 5, or 14 to select the Diffie-Hellman group to propose for Phase 2 of the IPSec VPN connection. Both VPN peers must use the same DH Group. | 5 |

| Variable | Description | Default |
|-------------------------------|---|-------------|
| dst-addr-type <type> | <p>Enter the type of destination address that corresponds to the recipient(s) or network behind the remote VPN peer or FortiGate dialup client:</p> <ul style="list-style-type: none"> To specify the IPv4 IP address of a server or host, type <code>ip</code>. Enter the IP address using the <code>dst-start-ip</code> field. To specify the IPv6 IP address of a server or host, type <code>ip6</code>. Enter the IP address using the <code>dst-start-ip6</code> field. To specify a range of IPv4 IP addresses, type <code>range</code>. Enter the starting and ending addresses using the <code>dst-start-ip</code> and <code>dst-end-ip</code> fields. To specify a range of IPv6 IP addresses, type <code>range6</code>. Enter the starting and ending addresses using the <code>dst-start-ip6</code> and <code>dst-end-ip6</code> fields. To specify an IPv4 network address, type <code>subnet</code>. Enter the network address using the <code>dst-subnet</code> field. To specify an IPv6 network address, type <code>subnet6</code>. Enter the network address using the <code>dst-subnet</code> field. To specify an address defined in a firewall address or address group, type <code>name</code>. Enter the address name using the <code>dst-name</code> field. You must also select the <code>name</code> option for <code>src-addr-type</code>. This is available only for IPv4 addresses. You should not use this option if <code>ike-version</code> is 1. IKEv1 does not support the use of multiple addresses in selectors. Instead, use the default 0.0.0.0/0 subnet selector and rely on the firewall policy to limit destination addresses. <p>This field is not available if <code>phase1name</code> names a configuration that enables <code>mode-cfg</code>.</p> | subnet |
| dst-end-ip <address_ipv4> | <p>This field is available when <code>dst-addr-type</code> is set to <code>range</code>. This field is not available if <code>phase1name</code> names a configuration that enables <code>mode-cfg</code>.</p> <p>Enter the highest destination IP address in the range of IP addresses.</p> | 0.0.0.0 |
| dst-end-ip6 <address_ipv6> | <p>This field is available when <code>dst-addr-type</code> is set to <code>range6</code>. This field is not available if <code>phase1name</code> names a configuration that enables <code>mode-cfg</code>.</p> <p>Enter the highest destination IP address in the range of IP addresses.</p> | :: |
| dst-name <address_name> | <p>This field is available when <code>dst-addr-type</code> is set to <code>name</code>. This field is not available if <code>phase1name</code> names a configuration that enables <code>mode-cfg</code>.</p> <p>Enter the firewall address or address group name.</p> | No default. |

| Variable | Description | Default |
|--|--|--------------------|
| dst-port <dest_port_number> | Enter the port number that the remote VPN peer or FortiGate dialup client uses to transport traffic related to the specified service (see <code>protocol</code>). The range is 1 to 65535. To specify all ports, type 0. This field is not available if <code>phase1name</code> names a configuration that enables <code>mode-cfg</code> . | 0 |
| dst-start-ip <address_ipv4> | This field is available when <code>dst-addr-type</code> is set to <code>range</code> . This field is not available if <code>phase1name</code> names a configuration that enables <code>mode-cfg</code> . Enter the lowest destination IP address in the range of IP addresses. | 0.0.0.0 |
| dst-start-ip6 <address_ipv6> | This field is available when <code>dst-addr-type</code> is set to <code>range6</code> . This field is not available if <code>phase1name</code> names a configuration that enables <code>mode-cfg</code> . Enter the lowest destination IP address in the range of IP addresses. | :: |
| dst-subnet <address_ipv4mask> | Enter the IPv4 IP address and network mask that identifies the private network behind the remote VPN peer or FortiGate dialup client. This field is not available if <code>phase1name</code> names a configuration that enables <code>mode-cfg</code> . | 0.0.0.0 0.0.0.0 |
| dst-subnet6 <address_ipv6mask> | Enter the IPv6 IP address and network mask that identifies the private network behind the remote VPN peer or FortiGate dialup client. This field is not available if <code>phase1name</code> names a configuration that enables <code>mode-cfg</code> . | ::/0 |
| encapsulation { tunnel-mode transport-mode } | Select encapsulation: <code>tunnel-mode</code> — Encrypt both payload data and headers. <code>transport-mode</code> — Encrypt only the payload data. This is used when combining IPsec with another encapsulation, such as GRE. | tunnel-mode |
| keepalive { enable disable } | Enable to automatically negotiate a new phase 2 security association (SA) before the current SA expires, keeping the tunnel up. Otherwise, a new SA is negotiated only if there is traffic. | disable |

| Variable | Description | Default |
|--------------------------------|---|---------|
| keylife-type <keylife_type> | <p>Set when the phase 2 key expires. When the key expires, a new key is generated without interrupting service.</p> <ul style="list-style-type: none"> To make the key expire after a period of time has expired and after an amount of data is transmitted, type <code>both</code>. To make the key expire after an amount of data is transmitted, type <code>kbs</code>. Use the <code>keylifekbs</code> field to set the amount of data that is transmitted. To make the key expire after a number of seconds elapses, type <code>seconds</code>. Use the <code>keylifeseconds</code> field to set the amount of time that elapses. | seconds |
| keylifekbs <kb_integer> | <p>This field is available when <code>keylife-type</code> is set to <code>kbs</code> or <code>both</code>.</p> <p>Set the number of KBits of data to transmit before the phase 2 key expires. The range is 5120 to 4 294 967 295 KBits.</p> | 5120 |
| keylifeseconds <seconds> | <p>This field is available when <code>keylife-type</code> is set to <code>seconds</code> or <code>both</code>.</p> <p>Set the number of seconds to elapse before the phase 2 key expires. <code>seconds</code> can be 120 to 172800 seconds.</p> | 1800 |
| l2tp {enable disable} | Enable L2TP traffic through this VPN. This is available if <code>encapsulation</code> is <code>transport-mode</code> and the <code>phase 1 type</code> is <code>dynamic</code> . | disable |
| pfs {enable disable} | Optionally, enable or disable perfect forward secrecy (PFS). PFS ensures that each key created during Phase 2 is unrelated to keys created during Phase 1 or to other keys created during Phase 2. PFS may cause minor delays during key generation. | enable |
| phase1name <gateway_name> | Enter a phase 1 gateway configuration name. You must add the phase 1 gateway definition to the FortiGate configuration before it can be cross-referenced. | Null. |

| Variable | Description | Default |
|--------------------------------|---|----------------------------------|
| proposal <encrypt_digest> | <p>Enter a minimum of one and a maximum of three encryption-message digest combinations (for example, 3des-md5). The remote peer must be configured to use at least one of the proposals that you define. Use a space to separate the combinations.</p> <p>You can enter any encryption-message digest combination except <code>null-null</code>.</p> <p>Here is an explanation of the abbreviated encryption algorithms:</p> <ul style="list-style-type: none"> • <code>null</code> — Do not use an encryption algorithm. • <code>des</code> — Digital Encryption Standard, a 64-bit block algorithm that uses a 56-bit key. • <code>3des</code> — Triple-DES, which encrypts data three times by three keys. • <code>aes128</code> — A 128-bit block algorithm that uses a 128-bit key. • <code>aes192</code> — A 128-bit block algorithm that uses a 192-bit key. • <code>aes256</code> — A 128-bit block algorithm that uses a 256-bit key. • <code>aria128</code> — A 128-bit Korean block algorithm that uses a 128-bit key. • <code>aria192</code> — A 128-bit Korean block algorithm that uses a 192-bit key. • <code>aria256</code> — A 128-bit Korean block algorithm that uses a 256-bit key. • <code>seed</code> — A 128-bit Korean block algorithm that uses a 128-bit key. <p>The ARIA and seed algorithms are not available on some models.</p> <p>You can enter any of the following message digests to check the authenticity of messages during an encrypted session:</p> <ul style="list-style-type: none"> • <code>null</code> — Do not use a message digest. • <code>md5</code> — Message Digest 5, the hash algorithm developed by RSA Data Security. • <code>sha1</code> — Secure Hash Algorithm 1, which produces a 160-bit message digest. • <code>sha256</code> — Secure Hash Algorithm 2, which produces a 256-bit message digest. | <p>aes128-sha1 3des-sha1</p> |
| protocol <protocol_integer> | <p>This field is available when <code>selector</code> is set to <code>specify</code>.</p> <p>Enter the IP protocol number for the service. The range is 1 to 255. To specify all services, type 0.</p> | 0 |

| Variable | Description | Default |
|----------------------------------|--|---------|
| replay {disable enable} | <p>Optionally, enable or disable replay detection. Replay attacks occur when an unauthorized party intercepts a series of IPSec packets and replays them back into the tunnel. Enable replay detection to check the sequence number of every IPSec packet to see if it has been received before. If packets arrive out of sequence, the FortiGate unit discards them.</p> <p>You can configure the FortiGate unit to send an alert email when it detects a replay packet. See “alertemail” on page 55.</p> | enable |
| route-overlap {overlap_option} | <p>Specify how FortiGate unit handles multiple dialup users with the same IP source address. Set <code>overlap_option</code> to one of the following:</p> <ul style="list-style-type: none">• <code>allow</code> — allow overlapping routes• <code>use-new</code> — delete the old route and add the new route• <code>use-old</code> — use the old route and do not add the new route | use-new |
| single-source {disable enable} | Enable or disable all FortiClient dialup clients to connect using the same phase 2 tunnel definition. | disable |

| Variable | Description | Default |
|-----------------------------------|---|---------|
| src-addr-type <ip_source_name> | <p>If the FortiGate unit is a dialup server, enter the type of source address that corresponds to the local sender(s) or network behind the FortiGate dialup server:</p> <ul style="list-style-type: none"> To specify the IPv4 IP address of a server or host, type <code>ip</code>. Enter the IP address using the <code>src-start-ip</code> field. To specify the IPv6 IP address of a server or host, type <code>ip6</code>. Enter the IP address using the <code>src-start-ip6</code> field. To specify a range of IPv4 IP addresses, type <code>range</code>. Enter the starting and ending addresses using the <code>src-start-ip</code> and <code>src-end-ip</code> fields. To specify a range of IPv6 IP addresses, type <code>range6</code>. Enter the starting and ending addresses using the <code>src-start-ip6</code> and <code>src-end-ip6</code> fields. To specify an IPv4 network address, type <code>subnet</code>. Enter the network address using the <code>src-subnet</code> field. To specify an IPv6 network address, type <code>subnet6</code>. Enter the network address using the <code>src-subnet6</code> field. To specify an address defined in a firewall address or address group, type <code>name</code>. Enter the address name using the <code>src-name</code> field. You must also select the <code>name</code> option for <code>dst-addr-type</code>. This is available only for IPv4 addresses. You should not use this option if <code>ike-version</code> is 1. IKEv1 does not support the use of multiple addresses in selectors. Instead, use the default 0.0.0.0/0 subnet selector and rely on the firewall policy to limit source addresses. <p>If the FortiGate unit is a dialup client, <code>src-addr-type</code> must refer to the server(s), host(s), or private network behind the FortiGate dialup client.</p> <p>This field is not available if <code>phase1name</code> names a configuration that enables <code>mode-cfg</code>.</p> | subnet |
| src-end-ip <address_ipv4> | <p>This field is available when <code>src-addr-type</code> is set to <code>range</code>. This field is not available if <code>phase1name</code> names a configuration that enables <code>mode-cfg</code>.</p> <p>Enter the highest source IP address in the range of IP addresses.</p> | 0.0.0.0 |
| src-end-ip6 <address_ipv6> | <p>This field is available when <code>src-addr-type</code> is set to <code>range6</code>. This field is not available if <code>phase1name</code> names a configuration that enables <code>mode-cfg</code>.</p> <p>Enter the highest source IP address in the range of IP addresses.</p> | :: |

| Variable | Description | Default |
|-----------------------------------|--|--------------------|
| src-name <address_name> | This field is available when <code>src-addr-type</code> is set to <code>name</code> . This field is not available if <code>phase1name</code> names a configuration that enables <code>mode-cfg</code> . Enter the firewall address or address group name. | |
| src-port <src_port_number> | If the FortiGate unit is a dialup server, enter the port number that the FortiGate dialup server uses to transport traffic related to the specified service (see <code>protocol</code>). If the FortiGate unit is a dialup client, enter the port number that the FortiGate dialup client uses to transport traffic related to the specified service. The <code>src-port</code> range is 1 to 65535. To specify all ports, type 0. This field is not available if <code>phase1name</code> names a configuration that enables <code>mode-cfg</code> . | 0 |
| src-start-ip <address_ipv4> | This field is available when <code>src-addr-type</code> is set to <code>range</code> . This field is not available if <code>phase1name</code> names a configuration that enables <code>mode-cfg</code> . Enter the lowest source IP address in the range of IP addresses. | 0.0.0.0 |
| src-start-ip6 <address_ipv6> | This field is available when <code>src-addr-type</code> is set to <code>range6</code> . This field is not available if <code>phase1name</code> names a configuration that enables <code>mode-cfg</code> . Enter the lowest source IP address in the range of IP addresses. | :: |
| src-subnet <address_ipv4mask> | If the FortiGate unit is a dialup server, enter the IPv4 IP address and network mask that identifies the private network behind the FortiGate dialup server. If the FortiGate unit is a dialup client, enter the IP address and network mask that identifies the private network behind the FortiGate dialup client. This field is not available if <code>phase1name</code> names a configuration that enables <code>mode-cfg</code> . | 0.0.0.0 0.0.0.0 |
| src-subnet6 <address_ipv6mask> | If the FortiGate unit is a dialup server, enter the IPv6 IP address and network mask that identifies the private network behind the FortiGate dialup server. If the FortiGate unit is a dialup client, enter the IP address and network mask that identifies the private network behind the FortiGate dialup client. This field is not available if <code>phase1name</code> names a configuration that enables <code>mode-cfg</code> . | ::/0 |

l2tp

Use this command to enable L2TP and specify a local address range to reserve for remote L2TP clients. When a remote L2TP client connects to the internal network through a L2TP VPN, the client is assigned an IP address from the specified range.

L2TP clients must authenticate with the FortiGate unit when a L2TP session starts. To support L2TP authentication on the FortiGate unit, you must define the L2TP users who need access and then add them to a user group. For more information, see [“user group” on page 722](#), [“user ldap” on page 726](#), [“user local” on page 729](#), and [“user radius” on page 735](#).

You need to define a firewall policy to control services inside the L2TP tunnel. For more information, see [“firewall” on page 99](#). When you define the firewall policy:

- Create an “external -> internal” policy.
- Set the source address to match the L2TP address range.
- Set the destination address to reflect the private address range of the internal network behind the local FortiGate unit.
- Set the policy service(s) to match the type(s) of traffic that L2TP users may generate.
- Set the policy action to `accept`.
- Enable NAT if required.



FortiGate units support L2TP with Microsoft Point-to-Point Encryption (MPPE) encryption only. Later implementations of Microsoft L2TP for Windows use IPsec and require certificates for authentication and encryption. If you want to use Microsoft L2TP with IPsec to connect to a FortiGate unit, the IPsec and certificate elements must be disabled on the remote client. For more information, see the [Disabling Microsoft L2TP for IPsec](#) article in the Fortinet Knowledge Center.

Syntax

```
config vpn l2tp
    set eip <address_ipv4>
    set sip <address_ipv4>
    set status {enable | disable}
    set usrgroup <group_name>
end
```



You can configure L2TP VPNs on FortiGate units that run in NAT/Route mode. The commands are available in NAT/Route mode only. When you configure an L2TP address range for the first time, you must enter a starting IP address, an ending IP address, and a user group.

| Variable | Description | Default |
|--------------------|--|---------|
| eip <address_ipv4> | The ending IP address of the L2TP address range. | 0.0.0.0 |
| sip <address_ipv4> | The starting IP address of the L2TP address range. | 0.0.0.0 |

| Variable | Description | Default |
|---------------------------|--|---------|
| status {enable disable} | Enable or disable L2TP VPN. | disable |
| usrgrp <group_name> | <p>This field is available when status is set to enable.</p> <p>Enter the name of the user group for authenticating L2TP clients. The user group must be added to the FortiGate configuration before it can be specified here. For more information, see “user group” on page 722, “user ldap” on page 726, “user local” on page 729, and “user radius” on page 735.</p> | Null |

pptp

Use this command to enable PPTP and specify a local address range to reserve for remote PPTP clients. When a remote PPTP client connects to the internal network through a PPTP VPN, the client is assigned an IP address from the specified range or from the server defined in the PPTP user group.

PPTP clients must authenticate with the FortiGate unit when a PPTP session starts. To support PPTP authentication on the FortiGate unit, you must define the PPTP users who need access and then add them to a user group. For more information, see [“user group” on page 722](#), [“user ldap” on page 726](#), [“user local” on page 729](#), [“user radius” on page 735](#), [“user peer” on page 732](#), and [“user peergrp” on page 734](#).

You need to define a firewall policy to control services inside the PPTP tunnel. For more information, see [“firewall” on page 99](#). When you define the firewall policy:

- Create an “external -> internal” policy.
- Set the source address to match the PPTP address range.
- Set the destination address to reflect the private address range of the internal network behind the local FortiGate unit.
- Set the policy service(s) to match the type(s) of traffic that PPTP users may generate.
- Set the policy action to `accept`.
- Enable NAT if required.

When you intend to use the FortiGate unit as a PPTP gateway, you can select a PPTP client IP from a local address range or use the server defined in the PPTP user group. You select which method to use for IP address retrieval and, in the case of the user group server, provide the IP address and the user group.

The FortiGate unit retrieves the `Framed-IP-Address` (the actual IP address of the client) from the RADIUS accounting start/stop message when `ip-mode` is set to `usrgrp`.

Syntax

```
config vpn pptp
    set eip <address_ipv4>
    set ip-mode {range | usrgrp}
    set local-ip <address_localip>
    set sip <address_ipv4>
    set status {enable | disable}
    set usrgrp <group_name>
end
```



You can configure PPTP VPNs on FortiGate units that run in NAT/Route mode. The commands are available in NAT/Route mode only. When you configure a PPTP address range for the first time, you must enter a starting IP address, an ending IP address, and a user group.

| Variable | Description | Default |
|----------------------------|---|---------|
| eip <address_ipv4> | The ending address of the PPTP address range. | 0.0.0.0 |
| ip-mode {range usrgrp} | Select one of: range — Assign user IP addresses from the IP address range of configured by sip and eip. usrgrp — Retrieve the IP address from the user group used to authenticate the user. Select the user group in usrgrp. | range |
| local-ip <address_localip> | Enter the IP address to be used for the peer's remote IP on the PPTP client side. | 0.0.0.0 |
| sip <address_ipv4> | The starting address of the PPTP IP address range. | 0.0.0.0 |
| status {enable disable} | Enable or disable PPTP VPN. | disable |
| usrgrp <group_name> | This field is available when ip-mode is set to usrgrp. Enter the name of the user group for authenticating PPTP clients. The user group must be added to the FortiGate configuration before it can be specified here. For more information, see “user group” on page 722 , “user ldap” on page 726 , “user local” on page 729 , “user radius” on page 735 , “user peer” on page 732 , and “user peergrp” on page 734 | Null |

ssl settings

Use this command to configure basic SSL VPN settings including interface idle-timeout values and SSL encryption preferences. If required, you can also enable the use of digital certificates for authenticating remote clients.

You can optionally specify the IP address of any Domain Name Service (DNS) server and/or Windows Internet Name Service (WINS) server that resides on the private network behind the FortiGate unit. The DNS and/or WINS server will find the IP addresses of other computers whenever a connected SSL VPN user sends an email message or browses the Internet.

You can configure SSL VPNs on FortiGate units that run in NAT/Route mode. The commands are available in NAT/Route mode only.

Syntax

```
config vpn ssl settings
    set algorithm <cipher_suite>
    set allow-ssl-big-buffer {enable | disable}
    set allow-ssl-client-renegotiation {enable | disable}
    set allow-ssl-insert-empty-fragment {enable | disable}
    set auth-timeout <auth_seconds>
    set auto-tunnel-policy {enable | disable}
    set auto-tunnel-static-route {enable | disable}
    set deflate-compression-level <int>
    set deflate-min-data-size <int>
    set dns-server1 <address_ipv4>
    set dns-server2 <address_ipv4>
    set dns-suffix <domain_str>
    set force-two-factor-auth {enable | disable}
    set force-utf8-login {enable | disable}
    set http-compression {enable | disable}
    set http-only-cookie {enable | disable}
    set idle-timeout <idle_seconds>
    set port <port_int>
    set port-precedence {enable | disable}
    set reqclientcert {enable | disable}
    set route-source-interface {enable | disable}
    set servercert <server_cert_name>
    set sslv2 {enable | disable}
    set sslv3 {enable | disable}
    set sslvpn-enable {enable | disable}
    set tlsv1-0 {enable | disable}
    set tlsv1-1 {enable | disable}
    set tlsv1-2 {enable | disable}
    set tunnel-ip-pools <pool1_name ...pooln_name>
    set url-obscuration {enable | disable}
    set wins-server1 <address_ipv4>
    set wins-server2 <address_ipv4>
end
```


When you configure the timeout settings, if you set the authentication timeout (`auth-timeout`) to 0, then the remote client does not have to re-authenticate again unless they log out of the system. In order to fully take advantage of this setting, the value for `idle-timeout` has to be set to 0 also, so the client does not timeout if the maximum idle time is reached. If the `idle-timeout` is not set to the infinite value, the system will log out if it reaches the limit set, regardless of the `auth-timeout` setting.

Set the `sslvpn-enable` attribute to `enable` to view all possible settings. The `tunnel-ip-pools` field is required for tunnel-mode access only. All other fields are optional.

| Variable | Description | Default |
|--|---|---------|
| <code>algorithm</code> <cipher_suite> | This field is available when <code>sslvpn-enable</code> is set to <code>enable</code> . Enter one of the following options to determine the level of SSL encryption to use. The web browser on the remote client must be capable of matching the level that you specify: <ul style="list-style-type: none"> To use any cipher suite, type <code>low</code>. To use a 128-bit or greater cipher suite, type <code>default</code>. To use a cipher suite that is greater than 128 bits, type <code>high</code>. | default |
| <code>allow-ssl-big-buffer</code> {enable disable} | The default setting (disable) reduces memory use by 16kbytes per connection. | disable |
| <code>allow-ssl-client-renegotiation</code> {enable disable} | Enable or disable renegotiation if tunnel goes down. SSL renegotiation feature could be used for DOS attack. | disable |
| <code>allow-ssl-insert-empty-fragment</code> {enable disable} | Internet Explorer 6 and earlier might not work well with the default setting (enable). The setting can be changed, but reduces security. | enable |
| <code>auth-timeout</code> <auth_seconds> | This field is available when <code>sslvpn-enable</code> is set to <code>enable</code> . Enter the period of time (in seconds) to control how long an authenticated connection will remain connected. When this time expires, the system forces the remote client to authenticate again. Range is 10 to 259,200 seconds (3 days). Use the value of 0 to indicate no timeout. | 28800 |
| <code>auto-tunnel-policy</code> {enable disable} | If enabled, when you add an SSL VPN portal with tunnel mode enabled, FortiOS automatically adds an SSL VPN tunnel policy so that you don't have to add one manually. | enable |
| <code>auto-tunnel-static-route</code> {enable disable} | If enabled, when you add an SSL VPN portal with tunnel mode enabled, FortiOS automatically adds static routes for the networks that can be accessed through the SSL VPN tunnel so that you don't have to add them manually. | enable |
| <code>deflate-compression-level</code> <int> | Set the compression level. Range is 1 (least compression) to 9 (most compression). Higher compression reduces the volume of data but requires more processing time. This field is available when <code>http-compression</code> is enabled. | 6 |

| Variable | Description | Default |
|---|---|---------|
| deflate-min-data-size <int> | Set the minimum amount of data that will trigger compression. Smaller amounts are not compressed. Range is 200 to 65 535 bytes. This field is available when <code>http-compression</code> is enabled. | 300 |
| dns-server1 <address_ipv4> | Enter the IP address of the primary DNS server that SSL VPN clients will be able to access after a connection has been established. If required, you can specify a secondary DNS server through the <code>dns-server2</code> attribute. | 0.0.0.0 |
| dns-server2 <address_ipv4> | Enter the IP address of a secondary DNS server if required. | 0.0.0.0 |
| dns-suffix <domain_str> | Enter the DNS suffix. Maximum length 253 characters. | null |
| force-two-factor-auth {enable disable} | Enable to require PKI (peer) users to authenticate by password in addition to certificate authentication. If this is enabled, only PKI users with two-factor authentication enabled will be able to log on to the SSL VPN. | disable |
| force-utf8-login {enable disable} | Enable to use UTF-8 encoding for the login page. This might be necessary when using LDAP to authenticate users. | disable |
| http-compression {enable disable} | Enable use of compression between the FortiGate unit and the client web browser. You can adjust the fields <code>deflate-compression-level</code> and <code>deflate-min-data-size</code> to tune performance. | disable |
| http-only-cookie {enable disable} | Disable only if a web site is having trouble with the tunnel mode Java Applet. | enable |
| idle-timeout <idle_seconds> | This field is available when <code>sslvpn-enable</code> is set to enable. Enter the period of time (in seconds) to control how long the connection can remain idle before the system forces the remote user to log in again. The range is from 10 to 259 200 seconds. Use the value of 0 to indicate no timeout. | 300 |
| port <port_int> | Enter the SSL VPN access port. Range 1 - 65 535. The port is usable only when <code>sslvpn-enable</code> is set to enable. When vdoms are enabled, this setting is per VDOM. | 10443 |
| port-precedence {enable disable} | Enable to give SSLVPN higher priority than HTTPS if both are enabled on the same port. | enable |
| reqclientcert {enable disable} | This field is available when <code>sslvpn-enable</code> is set to enable. Disable or enable the use of group certificates for authenticating remote clients. The SSLVPN daemon will require a client certificate for all SSL VPN users regardless of policy. | disable |

| Variable | Description | Default |
|--|--|-------------|
| route-source-interface { enable disable } | This field is available when <code>sslvpn-enable</code> is set to enable. Enable to allow the SSL VPN connection to bypass routing and bind to the incoming interface. | disable |
| servercert <server_cert_name> | This field is available when <code>sslvpn-enable</code> is set to enable. Enter the name of the signed server certificate that the FortiGate unit will use to identify itself during the SSL handshake with a web browser when the web browser connects to the login page. The server certificate must already be loaded into the FortiGate configuration. If you do not specify a server certificate, the FortiGate unit offers its factory installed (self-signed) certificate from Fortinet to remote clients when they connect. | self-sign |
| ssl2 { enable disable } | This field is available when <code>sslvpn-enable</code> is set to enable. Disable or enable SSL version 2 encryption. | disable |
| ssl3 { enable disable } | This field is available when <code>sslvpn-enable</code> is set to enable. Disable or enable SSL version 3 encryption. | enable |
| sslvpn-enable { enable disable } | Disable or enable remote-client access. | disable |
| tlsv1-0 { enable disable } | Enable or disable TLS 1.0 cryptographic protocol. | enable |
| tlsv1-1 { enable disable } | Enable or disable TLS 1.1 cryptographic protocol. | enable |
| tlsv1-2 { enable disable } | Enable or disable TLS 1.2 cryptographic protocol. | enable |
| tunnel-ip-pools <pool1_name ...pooln_name> | Enter the firewall addresses that represent the ranges of IP addresses reserved for remote clients. This field is available when <code>sslvpn-enable</code> is set to enable. | No default. |
| url-obscurtion { enable disable } | This field is available when <code>sslvpn-enable</code> is set to enable. Enable to encrypt the host name of the url in the display (web address) of the browser for web mode only. This is a requirement for ICSCA ssl vpn certification. Also, if enabled, bookmark details are not visible (field is blank.). | disable |
| wins-server1 <address_ipv4> | Enter the IP address of the primary WINS server that SSL VPN clients will be able to access after a connection has been established. If required, you can specify a secondary WINS server through the <code>wins-server2</code> attribute. | 0.0.0.0 |
| wins-server2 <address_ipv4> | Enter the IP address of a secondary WINS server if required. | 0.0.0.0 |

ssl web host-check-software

Use this command to define security software for selection in the `host-check-policy` field of the `vpn ssl web portal` command.

Syntax

```
config vpn ssl web host-check-software
edit <software_name>
    set guid <guid>
    set type {av | fw}
    set version <version_str>
config check-item-list
    edit <id_int>
        set action {deny | require}
        set md5s <md5_str>
        set target {file | process | registry}
        set type {file | process | registry}
        set version <version-str>
    end
end
```

| Variable | Description | Default |
|----------------------------------|---|-------------|
| <software_name> | Enter a name to identify the software. The name does not need to match the actual application name. | |
| set guid <guid> | Enter the globally unique identifier (GUID) for the host check application. The GUID is usually in the form xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx, where each x is a hexadecimal digit. Windows uses GUIDs to identify applications in the Windows Registry. | No default. |
| set type {av fw} | Select the software type: antivirus (av) or firewall (fw). If the software does both, create two entries, one where type is av and one where type is fw. | av |
| set version <version_str> | Enter the software version. | No default. |
| check-item-list variables | | |
| <id_int> | Enter an ID number for this entry. | |
| set action {deny require} | <p>Select one of</p> <p>require — If the item is found, the client meets the check item condition.</p> <p>deny — If the item is found, the client is considered to not meet the check item condition. Use this option if it is necessary to prevent use of a particular security product.</p> | require |
| set md5s <md5_str> | If type is <code>file</code> or <code>process</code> , enter one or more known MD5 signatures for the application executable file. You can use a third-party utility to calculate MD5 signatures or hashes for any file. You can enter multiple signatures to match multiple versions of the application. | |

| Variable | Description | Default |
|---|--|-------------|
| set target {file process registry} | <p>Enter information as follows:</p> <p>If type is <code>file</code>, enter the full path to the file.</p> <p>If type is <code>process</code>, enter the application's executable file name.</p> <p>If type is <code>registry</code>, enter the registry item.</p> | No default. |
| set type {file process registry} | <p>Select how to check for the application:</p> <ul style="list-style-type: none"> <code>file</code> — Look for a file. This could be the application's executable file or any other file that would confirm the presence of the application. Set <code>target</code> to the full path to the file. Where applicable, you can use environment variables enclosed in percent (%) marks. For example, <code>%ProgramFiles%\Fortinet\FortiClient\FortiClient.exe</code>. <code>process</code> — Look for the application as a running process. Set <code>target</code> to the application's executable file name. <code>registry</code> — Search for a Windows Registry entry. Set <code>target</code> to the registry item, for example <code>HKLM\SOFTWARE\Fortinet\FortiClient\Misc</code>. | file |
| set version <version-str> | Enter the version of the application. | No default. |

ssl web portal

The SSL VPN Service portal allows you to access network resources through a secure channel using a web browser. FortiGate administrators can configure log in privileges for system users and which network resources are available to the users, such as HTTP/HTTPS, telnet, FTP, SMB/CIFS, VNC, RDP and SSH.

The portal configuration determines what the system user sees when they log in to the FortiGate. Both the system administrator and the system user have the ability to customize the SSL VPN portal.

There are three pre-defined default web portal configurations available:

- *full-access*: Includes all widgets available to the user - *Session Information*, *Connection Tool*, *Bookmarks*, and *Tunnel Mode*.
- *tunnel-access*: Includes *Session Information* and *Tunnel Mode* widgets.
- *web-access*: Includes *Session Information* and *Bookmarks* widgets.

These pre-defined portal configurations can be edited, including their names.

Syntax

```
config vpn ssl web portal
  edit <portal_name>
    set allow-access <allow_access>
    set allow-user-bookmark {enable | disable}
    set auto-prompt-mobile-user-download {enable | disable}
    set cache-cleaner {enable | disable}
    set heading <str_heading>
    set host-check {av | av-fw | custom | fw | none}
    set host-check-interval <seconds>
    set host-check-policy <hcpolicy_name>
    set limit-user-logins {enable | disable}
    set mac-addr-action {allow | deny}
    set mac-addr-check {enable | disable}
    set os-check {enable | disable}
    set page-layout <double-column | single-column>
    set redir-url <redir_url>
    set skip-check-for-unsupported-browser {enable | disable}
    set skip-check-for-unsupported-os {enable | disable}
    set theme {blue | gray | orange}
    set virtual-desktop {enable | disable}
    set virtual-desktop-app-list <applist_name>
    set virtual-desktop-clipboard-share {enable | disable}
    set virtual-desktop-desktop-switch {enable | disable}
    set virtual-desktop-logout-when-browser-close
      {enable | disable}
    set virtual-desktop-network-share-access {enable | disable}
    set virtual-desktop-printing {enable | disable}
    set virtual-desktop-removable-media-access {enable | disable}
```

```
config mac-addr-check-rule
    edit <rule_name>
        set mac-addr-list <mac_list>
        set mac-addr-mask <int>
    end
config os-check-list {windows-2000 | windows-vista | windows-xp
    | windows-7 | windows-8}
    set action {allow | check-up-to-date | deny}
    set latest-patch-level {disable | 0 - 255}
    set tolerance {tolerance_num}
end
config widget
    edit id <widget_id>
        set name <name_str>
        set type <widget_type>
        set auto-connect {enable | disable}
        set column <column_number>
        set collapse {enable | disable}
        set dns-server1 <ip4_addr>
        set dns-server2 <ip4_addr>
        set allow-apps <service_type_access>
        set exclusive-routing {enable | disable}
        set ip-mode {range | usrgroup}
        set ip-pools {<pool1_name> .. <pooln_name>}
        set ipv6-dns-server1 <ip6_addr>
        set ipv6-dns-server2 <ip6_addr>
        set ipv6-wins-server1 <ip6_addr>
        set ipv6-wins-server2 <ip6_addr>
        set keep-alive {enable | disable}
        set save-password {enable | disable}
        set split-tunneling {enable | disable}
        set split-tunneling-routing-address <address_name>
        set wins-server1 <ip4_addr>
        set wins-server2 <ip4_addr>
    config bookmarks
        edit <bookmark_name>
            set additional-params <param_str>
            set apptype <service_type>
            set url <target_ip>
            set host <host_name>
            set folder <folder_name>
            set description <description_txt>
            set full-screen-mode {enable | disable}
            set keyboard-layout <locale_str>
            set listening-port <port_int>
            set logon-user <user-name_str>
            set logon-password <password_str>
            set remote-port <port_int>
            set screen-height <h_int>
```

```

set screen-width <w_int>
set show-status-window {enable | disable}
set sso {disable | auto}
set sso-credential {sslvpn-login | alternative}
set sso-password <pwd_str>
set sso-username <name_str>
end
end
end
end
end
end

```

| Variable | Description | Default |
|--|--|-------------|
| edit <portal_name_str> | Enter a name for the portal. Three pre-defined web portal configurations exist: full-access, tunnel-access, and web-access. | No default. |
| allow-access <allow_access> | Enter a list of the applications allowed in this portal. Separate entries with spaces. Application names are: <ul style="list-style-type: none"> • citrix for Citrix web server interface • ftp for FTP services. • ping for pinging hosts. • portforward for port forwarding. • rdp for Windows Terminal services. • rdpnative for remote desktop access with native client. • smb for SMB/CIFS (Windows file share) services. • ssh for SSH services. • telnet for telnet services. • vnc for VNC services. • web for HTTP and/or HTTPS services. | No default. |
| allow-user-bookmark {enable disable} | Allow web portal users to create their own bookmarks. | enable |
| auto-prompt-mobile-user-download {enable disable} | Enable to prompt mobile users to download FortiClient Endpoint Security. | enable |
| cache-cleaner {enable disable} | Enable the FortiGate unit to remove residual information from the remote client computer just before the SSL VPN session ends. This is done with a downloaded ActiveX control or | disable |
| heading <str_heading> | Enter the caption that appears at the top of the web portal home page. | null |

| Variable | Description | Default |
|--|--|---------------|
| host-check { av av-fw custom fw none } | Select the type of host checking to perform on endpoints: av — Check for antivirus software recognized by the Windows Security Center. av-fw — Check for both antivirus and firewall software recognized by the Windows Security Center. custom — Check for the software defined in host-check-policy. fw — Check for firewall software recognized by the Windows Security Center. none — Do not perform host checking. | none |
| host-check-interval <seconds> | Enter how often to recheck the host. Range is every 120 seconds to 259 200 seconds. Enter 0 to not recheck the host during the session. This is not available if host-check is none. | 0 |
| host-check-policy <hcpolicy_name> | Select the specific host check software to look for. These applications are defined in the vpn ssl web host-check-software command. This field is available when host-check is custom. | null |
| limit-user-logins { enable disable } | Enable to allow each user one SSL VPN session at a time. | disable |
| mac-addr-action { allow deny } | Set action for MAC address check: allow or deny connection. | allow |
| mac-addr-check { enable disable } | Enable or disable MAC address host check. | disable |
| os-check { enable disable } | Enable the FortiGate unit to determine what action to take depending on what operating system the client has. | disable |
| page-layout <double-column single-column> | Select the number of columns in the portal display. | single-column |
| redir-url <redir_url> | Enter the URL of the web page which will enable the FortiGate unit to display a second HTML page in a popup window when the web portal home page is displayed. The web server for this URL must reside on the private network behind the FortiGate unit. | null |
| skip-check-for-unsupported-browser { enable disable } | Skip the host check if the browser doesn't support it. This field is available if host checking is enabled. | enable |
| skip-check-for-unsupported-os { enable disable } | Skip the host check if the client operating system doesn't support it. This field is available if host checking is enabled. | enable |
| theme { blue gray orange } | Select the portal display theme (color). | blue |
| virtual-desktop { enable disable } | Enable the SSL VPN virtual desktop client application. If set to enable on the client, attempts to connect via SSL VPN are refused. | disable |

| Variable | Description | Default |
|--|---|------------------------|
| virtual-desktop-app-list <applist_name> | Enter the name of the application list to apply to the virtual desktop. See vpn ssl web virtual-desktop-app-list . | Null |
| virtual-desktop-clipboard-share {enable disable} | Enable or disable sharing of the clipboard with the regular desktop. | disable |
| virtual-desktop-desktop-switch {enable disable} | Enable or disable switching between virtual and regular desktop. | disable |
| virtual-desktop-logout-when-browser-close {enable disable} | Enable or disable automatic logout from virtual desktop when browser is closed. | disable |
| virtual-desktop-network-share-access {enable disable} | Enable or disable network share access from the virtual desktop. | disable |
| virtual-desktop-printing {enable disable} | Enable or disable printing from the virtual desktop. | disable |
| virtual-desktop-removable-media-access {enable disable} | Enable or disable accessing removable media such as USB drives from the virtual desktop. | disable |
| config mac-addr-check-rule variables | | |
| edit <rule_name> | Enter a name for this MAC check rule. | |
| mac-addr-list <mac_list> | Enter client MAC addresses. | No default. |
| mac-addr-mask <int> | Set the size of the netmask in bits. Range 1-48. | 48 |
| config os-check-list variables | | |
| Available when <code>set os-check</code> is set to <code>check-up-to-date</code> . | | |
| action {allow check-up-to-date deny} | Specify how to perform the patch level check. <ul style="list-style-type: none"> <code>allow</code> - any level is permitted <code>check-up-to-date</code> - some patch levels are permitted, make selections for <code>latest-patch-level</code> and <code>tolerance</code> <code>deny</code> - do not permit access for any version of this OS | allow |
| latest-patch-level {disable 0 - 255} | Specify the latest allowed patch level. Available when <code>action</code> is set to <code>enable</code> . | Win2000: 4 WinXP: 2 |
| tolerance {tolerance_num} | Specify the lowest allowable patch level tolerance. Equals <code>latest-patch-level</code> minus <code>tolerance</code> and above. Available when <code>action</code> is <code>check-up-to-date</code> . | 0 |
| Widget variables | | |
| id <widget_id> | Enter the unique ID number of the widget. | No default. |
| name <name_str> | Enter the name for the widget. Maximum 36 characters. | null |
| type <widget_type> | Enter the type of widget: bookmark, forticlient-download, history, info, tool or tunnel. | bookmark |
| auto-connect {enable disable} | Enable or disable FortiClient automatic connection to this portal. | disable |

| Variable | Description | Default |
|--|--|--------------------|
| column <column_number> | Enter the number of columns in the widget display: one or two. This is available if <code>page-layout</code> is <code>double-column</code> . | one |
| collapse {enable disable} | Enable the widget to expand in the web portal view. Allows user to make changes to the widget view/configuration. | disable |
| dns-server1 <ip4_addr> dns-server2 <ip4_addr> | Specify primary and secondary DNS servers. This is available if <code>type</code> is <code>tunnel</code> . | 0.0.0.0 0.0.0.0 |
| allow-apps <service_type_access> | If <code>type</code> is <code>bookmark</code> , select the types of bookmarks the user can create. If <code>type</code> is <code>tool</code> , select the types of services that the user can access with this widget. Separate entries with spaces. <ul style="list-style-type: none"> • <code>citrix</code> for Citrix web server interface • <code>ftp</code> for FTP services • <code>ping</code> for pinging hosts (tool only) • <code>portforward</code> for port forwarding • <code>rdp</code> for Windows Terminal services • <code>rdpnative</code> for remote desktop access with native client • <code>smb</code> for SMB/CIFS (Windows file share) services • <code>ssh</code> for SSH services • <code>telnet</code> for telnet services • <code>vnc</code> for VNC services • <code>web</code> for HTTP and/or HTTPS services | No default. |
| exclusive-routing {enable disable} | Enable to force traffic between the client and the client's local network to pass through the SSL VPN tunnel. This can enhance security. By default, an SSL VPN with <code>split-tunneling</code> disabled does not affect traffic between the client and the client's local network, even though all other traffic is routed through the SSL VPN tunnel. <code>exclusive-routing</code> is available only when <code>split-tunneling</code> is disabled. | disable |
| ip-mode {range usrgroup} | Select the mode by which the IP address is assigned to the user: Available only if <code>tunnel-status</code> is enabled. | range |
| ip-pools {<pool1_name> .. <pooln_name>} | Enter the names of the IP pools (firewall addresses) that represent IP address ranges reserved for tunnel-mode SSL VPN clients. This is available only if <code>tunnel-status</code> is enabled. | |

| Variable | Description | Default |
|--|---|--------------------|
| ipv6-dns-server1 <ip6_addr> ipv6-dns-server2 <ip6_addr> | Specify primary and secondary IPv6 DNS servers. This is available if <code>type</code> is <code>tunnel</code> . | :: :: |
| ipv6-wins-server1 <ip6_addr> ipv6-wins-server2 <ip6_addr> | Specify primary and secondary IPv6 WINS servers. This is available if <code>type</code> is <code>tunnel</code> . | :: :: |
| keep-alive {enable disable} | Enable or disable keepalive (automatic reconnect) for FortiClient connections to this portal. | |
| save-password {enable disable} | Enable or disable FortiClient saving of user password. | disable |
| split-tunneling {enable disable} | Enable split tunneling. Split tunneling ensures that only the traffic for the private network is sent to the SSL VPN gateway. Internet traffic is sent through the usual unencrypted route. Available only if <code>tunnel-status</code> is enabled. | disable |
| split-tunneling-routing-address <address_name> | Enter the firewall addresses for the destinations that clients will reach through the SSL VPN. The client's split-tunneling configuration will ensure that the tunnel is used for these destinations only. This is available when <code>split-tunneling</code> is enabled. | No default. |
| wins-server1 <ip4_addr> wins-server2 <ip4_addr> | Specify primary and secondary WINS servers. This is available if <code>type</code> is <code>tunnel</code> . | 0.0.0.0 0.0.0.0 |

| Variable | Description | Default |
|--|--|-------------|
| Bookmarks variables | | |
| Note: config bookmarks is available only when widget type is bookmark. | | |
| <bookmark_name> | Enter the unique name of the bookmark. Maximum 36 characters. | null |
| additional-params <param_str> | Enter additional parameters the application requires. Available when apptype is citrix, portforward, rdp, or rdpnative. | |
| apptype <service_type> | Enter the identifier of the service to associate with the bookmark: <ul style="list-style-type: none"> Type citrix for Citrix web server interface. Type ftp for FTP services. Type portforward for port forwarding. Type rdp for Windows Terminal services. Type rdpnative for remote desktop access with native client. Type smb for SMB/CIFS (Windows file share) services. Type ssh for SSH services. Type telnet for telnet services. Type vnc for VNC services. Type web for HTTP and/or HTTPS services. | web |
| url <target_ip> | Enter the URL of the web page, if apptype is web or citrix. | No default. |
| host <host_name> | Enter the host name, if apptype is telnet or rdp. Maximum 36 characters. | No default. |
| folder <folder_name> | Enter the remote folder name, if apptype is smb or ftp. The folder name must include the server name, //172.20.120.103/myfolder, for example. | No default. |
| description <description_txt> | Enter a description of the bookmark. Maximum 129 characters. | null |
| full-screen-mode {enable disable} | Enable or disable full-screen mode. Available when apptype is rdp or rdpnative. | disable |
| keyboard-layout <locale_str> | Enter the keyboard layout for the RDP session. Available when apptype is rdp. | en-us |
| listening-port <port_int> | Enter the listening port number. Available when apptype is portforward. | null |
| logon-user <user-name_str> logon-password <password_str> | Enter the logon credentials for the RDP bookmark. Available when apptype is rdp. | null |
| remote-port <port_int> | Enter the remote port number. Available when apptype is portforward. | null |

| Variable | Description | Default |
|--|---|--------------|
| screen-height <h_int> | Enter screen height in pixels. Available when apptype is rdp or rdpnative. | 768 |
| screen-width <w_int> | Enter screen width in pixels. Available when apptype is rdp or rdpnative. | 1024 |
| show-status-window {enable disable} | Enable or disable the status window. Available when apptype is portforward. | disable |
| sso {disable auto} | A Single Sign-On (SSO) bookmark automatically enters the login credentials for the bookmark destination. Select one of: disable — This is not an SSO bookmark. auto — SSO bookmark, configure sso-credential. | disable |
| sso-credential {sslvpn-login alternative} | Select whether the bookmark enters the user's SSL VPN credentials or alternative credentials defined in sso-username and sso-password. | sslvpn-login |
| sso-password <pwd_str> | Enter alternative password. Available when sso-credential is alternative. | No default. |
| sso-username <name_str> | Enter alternative username. Available when sso-credential is alternative. | No default. |

ssl web realm

Use this command to configure SSL VPN realms.

Syntax

```
config vpn ssl web realm
  edit <url-path>
    set login-page <content_str>
    set max-concurrent-user <int>
    set virtual-host <hostname_str>
  end
end
```

| Variable | Description | Default |
|-----------------------------|--|-------------|
| edit <url-path> | Enter the URL path to access the SSL-VPN login page. Do not include "http://". | No default. |
| login-page <content_str> | Enter replacement HTML for SSL-VPN login page. | No default. |
| max-concurrent-user <int> | Enter the maximum number of concurrent users allowed. Range 0-65 535. 0 means unlimited. | 0 |
| virtual-host <hostname_str> | Enter the virtual host name for this realm. Optional. Maximum length 255 characters. | No default. |

ssl web user

Use this command to configure SSL VPN users and their bookmarks.

Syntax

```
config vpn ssl web user
  edit <user_name>
    config widget
      edit <widget_id>
        config bookmarks
          edit <bookmark_name>
            set apptype <service_type>
            set description <description_txt>
            set sso {disable | auto}
            set sso-credential {sslvpn-login | alternative}
            set sso-password <pwd_str>
            set sso-username <name_str>
            set url <url_str>
            config form-data
              edit <id_int>
                set name <fieldname_str>
                set value <value_str>
              end
            end
          end
        end
      end
    end
  end
end
```

| Variable | Description | Default |
|----------------------------------|--|---------|
| <user_name> | Enter a name for the user. | |
| apptype <service_type> | Enter the identifier of the service to associate with the bookmark: <ul style="list-style-type: none"> Type <code>citrix</code> for Citrix web server interface. Type <code>ftp</code> for FTP services. Type <code>portforward</code> for port forwarding. Type <code>rdp</code> for Windows Terminal services. Type <code>rdpnative</code> for remote desktop access with native client. Type <code>smb</code> for SMB/CIFS (Windows file share) services. Type <code>ssh</code> for SSH services. Type <code>telnet</code> for telnet services. Type <code>vnc</code> for VNC services. Type <code>web</code> for HTTP and/or HTTPS services. | web |
| description <description_txt> | Enter a description of the bookmark. Maximum 129 characters. | null |

| Variable | Description | Default |
|--|---|--------------|
| sso {disable auto} | A Single Sign-On (SSO) bookmark automatically enters the login credentials for the bookmark destination. Select one of: disable — This is not an SSO bookmark. auto — SSO bookmark, configure <code>sso-credential</code> . static — SSO bookmark with form data. | disable |
| sso-credential {sslvpn-login alternative} | Select whether the bookmark enters the user's SSL VPN credentials or alternative credentials defined in <code>sso-username</code> and <code>sso-password</code> . | sslvpn-login |
| sso-password <pwd_str> | Enter alternative password. Available when <code>sso-credential</code> is <code>alternative</code> . | No default. |
| sso-username <name_str> | Enter alternative username. Available when <code>sso-credential</code> is <code>alternative</code> . | No default. |
| url <url_str> | Enter the URL for this bookmark. | No default. |
| config form-data variables These fields are available when <code>sso</code> is <code>static</code> . | | |
| edit <id_int> | Enter an identifier. | |
| name <fieldname_str> | Enter a required login page field name, "User Name" for example. | No default. |
| value <value_str> | Enter the value to enter in the field identified by <code>name</code> . If you are an administrator configuring a bookmark for users: Enter <code>%username%</code> to represent the user's SSL VPN user name. Enter <code>%passwd%</code> to represent the user's SSL VPN password. | No default. |

ssl web virtual-desktop-app-list

Use this command to create a list of either allowed or blocked applications which you then select when you configure the virtual desktop.

Syntax

```
config vpn ssl web virtual-desktop-app-list
  edit <applist_name>
    set set action {allow | block}
    config apps
      edit <app_name>
        set md5s <md5_str>
      end
    end
  end
end
```

| Variable | Description | Default |
|-------------------------------|--|-------------|
| <applist_name> | Enter a name for the application control list. | |
| set action {allow block} | Set the action for this application control list: allow — Allow the applications on this list and block all others. block — Block the applications on this list and allow all others | allow |
| <app_name> | Enter the name of the application to be added to the application control list. This can be any name and does not have to match the official name of the application. | |
| set md5s <md5_str> | Enter one or more known MD5 signatures (space-separated) for the application executable file. You can use a third-party utility to calculate MD5 signatures or hashes for any file. You can enter multiple signatures to match multiple versions of the application. | No default. |

wanopt

Use these commands to configure FortiGate WAN optimization.

[auth-group](#)

[peer](#)

[profile](#)

[settings](#)

[ssl-server](#)

[storage](#)

[webcache](#)

auth-group

Use this command to configure WAN optimization authentication groups. Add authentication groups to support authentication and secure tunneling between WAN optimization peers.

Syntax

```
config wanopt auth-group
  edit <auth_group_name>
    set auth-method {cert | psk}
    set cert <certificate_name>
    set peer <peer_host_id>
    set peer-accept {any | defined | one}
    set psk <preshared_key>
  end
```

| Variable | Description | Default |
|-----------------------------------|---|---------|
| edit <auth_group_name> | Enter a name for the authentication group. | |
| auth-method {cert psk} | Specify the authentication method for the authentication group. Enter <code>cert</code> to authenticate using a certificate. Enter <code>psk</code> to authenticate using a preshared key. | cert |
| cert <certificate_name> | If <code>auth-method</code> is set to <code>cert</code> , select the local certificate to be used by the peers in this authentication group. The certificate must be a local certificate added to the FortiGate unit using the <code>config vpn certificate local</code> command. For more information, see “vpn certificate local” on page 760 . | |
| peer <peer_host_id> | If <code>peer-method</code> is set to <code>one</code> select the name of one peer to add to this authentication group. The peer must have been added to the FortiGate unit using the <code>config wanopt peer</code> command. | |
| peer-accept {any defined one} | Specify whether the authentication group can be used for any peer, only the defined peers that have been added to the FortiGate unit configuration, or just one peer. If you specify one use the <code>peer</code> field to add the name of the peer to the authentication group. | any |
| psk <preshared_key> | If <code>auth-method</code> is set to <code>psk</code> enter a preshared key to be used for the authentication group. | |

peer

Add WAN optimization peers to a FortiGate unit to identify the FortiGate units that the local FortiGate unit can form WAN optimization tunnels with. A peer consists of a peer name, which is the local host ID of the remote FortiGate unit and an IP address, which is the IP address of the interface that the remote FortiGate unit uses to connect to the local FortiGate unit.

Use the command `config wanopt settings` to add the local host ID to a FortiGate unit.

Syntax

```
config wanopt peer
  edit <peer_name>
    set ip <peer_ip_ipv4>
  end
```

| Variable | Description | Default |
|-------------------|---|---------|
| edit <peer_name> | Add the local host ID of the remote FortiGate unit. When the remote FortiGate unit connects to the local FortiGate unit to start a WAN optimization tunnel, the WAN optimization setup request include the remote FortiGate unit local host ID. If the local host ID in the setup request matches a peer added to the local FortiGate unit, then the local FortiGate unit can accept WAN optimization tunnel setup requests from the remote FortiGate unit. | |
| ip <peer_ip_ipv4> | Enter the IP address of the interface that the remote FortiGate unit uses to connect to the local FortiGate unit. Usually this would be the IP address of the interface connected to the WAN. | 0.0.0.0 |

profile

WAN optimization uses profiles to select traffic to be optimized. But, before WAN optimization can accept traffic, the traffic must be accepted by a FortiGate firewall policy. All sessions accepted by a firewall policy that also match a WAN optimization profile are processed by WAN optimization.

To configure WAN optimization you add WAN optimization profiles to the FortiGate units at each end of the tunnel. Firewall policies use the specified WAN optimization profile to determine how to optimize the traffic over the WAN.

The FortiGate unit applies firewall policies to packets before WAN optimization profiles. A WAN optimization profile is applied to a packet only after the packet is accepted by a firewall policy.

Syntax

```
config wanopt profile
  edit <name_str>
    set auth-group <auth_group_name>
    set transparent {enable | disable}
    config {cifs | ftp | http | mapi | tcp}
      set byte-caching {enable | disable}
      set byte-caching-opt {mem-only | mem-disk}
      set log-traffic {enable | disable}
      set port <port_int>[-<port-int>]
      set prefer-chunking {fix | dynamic}
      set secure-tunnel {enable | disable}
      set ssl {enable | disable}
      set status {enable | disable}
      set tunnel-non-http {enable | disable}
      set tunnel-sharing {express-shared | private | shared}
      set unknown-http-version {best-effort | reject | tunnel}
    end
  end
```

| Variable | Description | Default |
|------------------------------|--|---------|
| edit <name_str> | Enter a name for this profile. | |
| auth-group <auth_group_name> | <p>Select an authentication group to be used by this profile. Select an authentication group if you want the client and server FortiGate units that use this profile to authenticate with each other before starting a WAN optimization tunnel.</p> <p>You must add the same authentication group to the client and server FortiGate units. The authentication group should have the same name of both FortiGate units and use the same pre-shared key or the same certificate.</p> <p>You can add an authentication group to profiles with auto-detect set to off or active. An authentication group is required if you enable secure-tunnel for the profile.</p> | |

| Variable | Description | Default |
|---|--|--|
| transparent {enable disable} | <p>Enable or disable transparent mode for this profile.</p> <p>If you enable transparent mode, WAN optimization keeps the original source address of the packets, so servers appear to receive traffic directly from clients. Routing on the server network should be able to route traffic with client IP addresses to the FortiGate unit.</p> <p>If you do not select transparent mode, the source address of the packets received by servers is changed to the address of the FortiGate unit interface. So servers appear to receive packets from the FortiGate unit. Routing on the server network is simpler in this case because client addresses are not involved, but the server sees all traffic as coming from the FortiGate unit and not from individual clients.</p> | enable |
| config {cifs ftp http mapi tcp} fields | | |
| byte-caching {enable disable} | Enable or disable WAN optimization byte caching for the traffic accepted by this profile. Byte caching is a WAN optimization technique that reduces the amount of data that has to be transmitted across a WAN by caching file data to serve it later as required. Byte caching is available for all protocols. | For TCP, disable For all others, enable |
| byte-caching-opt {mem-only mem-disk} | Select whether byte-caching optimization uses only memory or both memory and disk. This is available for TCP only. | mem-only |
| log-traffic {enable disable} | Enable or disable traffic logging. | enable |
| port <port_int>[-<port_int>] | Enter a single port number or port number range for the profile. Only packets whose destination port number matches this port number or port number range will be accepted by and subject to this profile. | 0 |
| prefer-chunking {fix dynamic} | <p>Select dynamic or fixed data chunking. Dynamic data chunking helps to detect persistent data chunks in a changed file or in an embedded unknown protocol.</p> <p>prefer-chunking is not available for TCP and MAPI.</p> <p>For TCP, if byte-caching-opt is mem-disk, chunking algorithm will be dynamic. For MAPI, only dynamic is used. For other protocols, fix is the default.</p> | Depends on protocol. |

| Variable | Description | Default |
|------------------------------------|---|---------|
| secure-tunnel {enable disable} | <p>Enable or disable using AES-128bit-CBC SSL to encrypt and secure the traffic in the WAN optimization tunnel. The FortiGate units use FortiASIC acceleration to accelerate SSL decryption and encryption of the secure tunnel. The secure tunnel uses the same TCP port as a non-secure tunnel (TCP port 7810).</p> <p>You can configure <code>secure-tunnel</code> if <code>auto-detect</code> is set to <code>active</code> or <code>off</code>. If you enable <code>secure-tunnel</code> you must also add an <code>auth-group</code> to the profile.</p> | disable |
| ssl {enable disable} | <p>Enable or disable applying SSL offloading for HTTPS traffic. You use SSL offloading to offload SSL encryption and decryption from one or more HTTP servers. If you enable <code>ssl</code>, you should configure the profile to accept SSL-encrypted traffic, usually by configuring the profile to accept HTTPS traffic by setting <code>port</code> to 443.</p> <p>If you enable SSL you must also use the <code>config wanopt ssl-server</code> command to add an SSL server for each HTTP server that you want to offload SSL encryption/decryption for. See “wanopt ssl-server” on page 843.</p> <p>You can configure <code>ssl</code> if <code>auto-detect</code> is set to <code>active</code> or <code>off</code>.</p> | disable |
| status {enable disable} | Enable or disable the profile. | enable |
| tunnel-non-http {enable disable} | <p>Configure how to process non-HTTP traffic when a profile configured to accept and optimize HTTP traffic accepts a non-HTTP session. This can occur if an application sends non-HTTP traffic using an HTTP destination port.</p> <p>Select <code>disable</code> to drop or tear down non-HTTP sessions accepted by the profile.</p> <p>Select <code>enable</code> to pass non-HTTP sessions through the tunnel without applying protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied to non-HTTP sessions.</p> <p>You can configure <code>tunnel-non-http</code> if <code>proto</code> is set to <code>http</code> and <code>auto-detect</code> is set to <code>active</code> or <code>off</code>.</p> | disable |

| Variable | Description | Default |
|--|---|---------|
| tunnel-sharing {express-shared private shared} | <p>Select the tunnel sharing mode for this profile:</p> <p>Select <code>express-shared</code> for profiles that accept interactive protocols such as Telnet.</p> <p>Select <code>private</code> for profiles that accept aggressive protocols such as HTTP and FTP so that these aggressive protocols do not share tunnels with less-aggressive protocols.</p> <p>Select <code>shared</code> for profiles that accept non-aggressive and non-interactive protocols.</p> <p>You can configure tunnel sharing if <code>proto</code> is set to <code>http</code> and <code>auto-detect</code> is set to <code>off</code>.</p> | private |
| unknown-http-version {best-effort reject tunnel} | <p>Unknown HTTP sessions are HTTP sessions that don't comply with HTTP 0.9, 1.0, or 1.1. Configure <code>unknown-http-version</code> to specify how a profile handles HTTP traffic that does not comply with HTTP 0.9, 1.0, or 1.1.</p> <p>Select <code>best-effort</code> to assume all HTTP sessions accepted by the profile comply with HTTP 0.9, 1.0, or 1.1. If a session uses a different HTTP version, WAN optimization may not parse it correctly. As a result the FortiGate unit may stop forwarding the session and the connection may be lost.</p> <p>Select <code>reject</code> to reject or tear down HTTP sessions that do not use HTTP 0.9, 1.0, or 1.1.</p> <p>Select <code>tunnel</code> to pass HTTP traffic that does not use HTTP 0.9, 1.0, or 1.1 without applying HTTP protocol optimization, byte-caching, or web caching. TCP protocol optimization is applied to this HTTP traffic.</p> <p>You can configure <code>unknown-http-version</code> if <code>proto</code> is set to <code>http</code> and <code>auto-detect</code> is set to <code>active</code> or <code>off</code>.</p> | tunnel |

settings

Use this command to add or change the FortiGate WAN optimization local host ID and to enable traffic logging for WAN optimization and WAN optimization web caching sessions. The local host ID identifies the FortiGate unit to other FortiGate units for WAN optimization. All WAN optimization tunnel startup requests to other FortiGate units include the local host id. The FortiGate unit can only perform WAN optimization with other FortiGate units that have this local host id in their peer list.

Syntax

```
config wanopt settings
    set host-id <host-id-name_str>
    set log-traffic {cifs ftp http mapi tcp}
    set tunnel-ssl-algorithm {high | medium | low}
end
```

| Variable | Description | Default |
|--|--|------------|
| host-id <host-id-name_str> | Enter the local host ID. | default-id |
| log-traffic {cifs ftp http mapi tcp} | Enable WAN optimization and WAN optimization web caching traffic logging for each type of WAN optimization session. Valid types are: cifs ftp http mapi tcp. Separate each type with a space. To add or remove an option from the list, retype the complete list as required. | |
| tunnel-ssl-algorithm {high medium low} | Select the relative strength of encryption accepted for SSL tunnel negotiation. high encryption allows AES and 3DES. medium encryption allows AES, 3DES, and RC4. low encryption allows AES, 3DES, RC4, and DES. | high |

ssl-server

Use this command to add one or more SSL servers to support WAN optimization SSL offloading. You enable WAN optimization SSL offloading by enabling the `ssl` field in a WAN optimization rule. WAN optimization supports SSL encryption/decryption offloading for HTTP servers.

SSL offloading uses the FortiGate unit to encrypt and decrypt SSL sessions. The FortiGate unit intercepts HTTPS traffic from clients and decrypts it before sending it as clear text to the HTTP server. The clear text response from the HTTP server is encrypted by the FortiGate unit and returned to the client. The result should be a performance improvement because SSL encryption is offloaded from the server to the FortiGate unit FortiASIC SSL encryption/decryption engine.

You must add one WAN optimization SSL server configuration to the FortiGate unit for each HTTP server that you are configuring SSL offloading for. This SSL server configuration must also include the HTTP server CA. You load this certificated into the FortiGate unit as a local certificate using the `config vpn certification local` command and then add the certificate to the SSL server configuration using the `ssl-cert` field. The certificate key size must be 1024 or 2048 bits. 4096-bit keys are not supported.

You can configure one WAN optimization rule to offload SSL encryption/decryption for multiple HTTP servers. To do this, the WAN optimization rule source and destination addresses must be configured so that the rule accepts packets destined for all of the HTTP servers that you want offloading for. Then you must add one SSL server configuration for each of the HTTP servers.

Syntax

```
config wanopt ssl-server
  edit <ssl-server-name>
    set add-header-x-forwarded-proto {enable | disable}
    set ip <ssl_server_ip_ipv4>
    set port <port_int>
    set ssl-mode {full | half}
    set ssl-algorithm {low | medium | high}
    set ssl-cert <certificate_name>
    set ssl-client-renegotiation {allow | deny | secure}
    set ssl-dh-bits {1024 | 1536 | 2048 | 768}
    set ssl-min-version {ssl-3.0 | tls-1.0}
    set ssl-max-version {ssl-3.0 | tls-1.0}
    set ssl-send-empty-frags {disable | enable}
    set url-rewrite {enable | disable}
  end
```

| Variable | Description | Default |
|---|--|---------|
| edit <ssl-server-name> | Enter a name for the SSL server. It can be any name and this name is not used by other FortiGate configurations. | |
| add-header-x-forwarded-proto {enable disable} | Optionally add X-Forwarded-Proto header. This is available when <code>ssl-mode</code> is <code>half</code> . | enable |

| Variable | Description | Default |
|---|--|---------|
| ip <ssl_server_ip_ipv4> | Enter an IP address for the SSL server. This IP address should be the same as the IP address of the HTTP server that this SSL server will be offloading for. When a session is accepted by a WAN optimization rule with SSL offloading enabled, the destination IP address of the session is matched with this IP address to select the SSL server configuration to use. | 0.0.0.0 |
| port <port_int> | Enter a port number to be used by the SSL server. Usually this would be port 443 for an HTTPS server. When a session is accepted by a WAN optimization rule with SSL offloading enabled, the destination port of the session is matched with this port to select the SSL server configuration to use. | 0 |
| ssl-mode {full half} | Configure the SSL server to operate in <code>full</code> mode or <code>half</code> mode. Half mode offloads SSL from the backend server to the server-side FortiGate unit. | full |
| ssl-algorithm {low medium high} | Set the permitted encryption algorithms for SSL sessions according to encryption strength: low — AES, 3DES, RC4, DES medium — AES, 3DES, RC4 high — AES, 3DES | high |
| ssl-cert <certificate_name> | Select the certificate to be used for this SSL server. The certificate should be the HTTP server CA used by the HTTP server that this SSL server configuration will be offloading for. The certificate must be a local certificate added to the FortiGate unit using the <code>config vpn certificate local</code> command. For more information, see “vpn certificate local” on page 760 . The certificate key size must be 1024 or 2048 bits. 4096-bit keys are not supported. | |
| ssl-client-renegotiation {allow deny secure} | Select whether client renegotiation is allowed. The <code>deny</code> option aborts any SSL connection that attempts to renegotiate. The <code>secure</code> option rejects any SSL connection that does not offer an RFC 5746 Secure Renegotiation Indication. | allow |
| ssl-dh-bits {1024 1536 2048 768} | Select the size of the Diffie-Hellman prime used in DHE_RSA negotiation. Larger primes may cause a performance reduction but are more secure. | 1024 |
| ssl-min-version {ssl-3.0 tls-1.0} | Select the lowest or oldest SSL/TLS version to offer when negotiating. You can set the minimum version to SSL 3.0 or TLS 1.0. TLS 1.0 is more secure than SSL 3.0. | ssl-3.0 |
| ssl-max-version {ssl-3.0 tls-1.0} | Select the highest or newest SSL/TLS version to offer when negotiating. You can set the maximum version to SSL 3.0 or TLS 1.0. TLS 1.0 is more secure than SSL 3.0. | tls-1.0 |

| Variable | Description | Default |
|---|--|---------|
| ssl-send-empty-frags {disable enable} | Enable or disable sending empty fragments before sending the actual payload. Sending empty fragments is a technique used to avoid cipher-block chaining (CBC) plaintext attacks if the initiation vector (IV) is known. Also called the CBC IV. Some SSL implementations are not compatible with sending empty fragments. Change <code>ssl-send-empty-frags</code> to <code>disable</code> if required by your SSL implementation. | enable |
| url-rewrite {enable disable} | Enable to rewrite Location header of HTTP redirection response(3XX response). This is available when <code>ssl-mode</code> is <code>half</code> . | disable |

storage

Use this command to change the size of WAN optimization storages. A storage defines the maximum size of the byte caching or web caching database added to the storage.

Syntax

```
config wanopt storage
  edit <storage_name_str>
    set size <partition_size_int>
    set webcache-storage-percentage <int>
  end
```

| Variable | Description | Default |
|-----------------------------------|---|---------|
| edit <storage_name_str> | Enter the name of a storage configured using the config system storage command. All FortiGate units with hard disks include a default storage name such as Internal or ASM. | |
| size <partition_size_int> | Enter the size of the partition in Mbytes. The default depends on the partition size. | |
| webcache-storage-percentage <int> | Enter the portion, in percent, of the storage that is used for web cache. Remainder is used for wanopt. | 50 |

webcache

Use this command to change how the WAN optimization web cache operates. In most cases the default settings are acceptable. However you may want to change these settings to improve performance or optimize the cache for your configuration.

Syntax

```
config wanopt webcache
  set always-revalidate {enable | disable}
  set always-revalidate {enable | disable}
  set cache-cookie {enable | disable}
  set cache-expired {enable | disable}
  set default-ttl <expiry_time>
  set fresh-factor <fresh_percent>
  set ignore-conditional {enable | disable}
  set ignore-ie-reload {enable | disable}
  set ignore-ims {enable | disable}
  set ignore-pnc {enable | disable}
  set max-object-size <object_size>
  set max-ttl <expiry_time>
  set min-ttl <expiry_time>
  set neg-resp-time <response_time>
  set reval-pnc {enable | disable}
end
```

| Variable | Description | Default |
|---|---|---------|
| always-revalidate {enable disable} | Enable to always to revalidate the requested cached object with content on the server before serving it to the client. | enable |
| cache-cookie {enable disable} | Enable caching of cookies. Typically a HTTP response with a cookie contains data for a specific user, so cookie caching is best not done. | disable |
| cache-expired {enable disable} | Applies only to type-1 objects. When this setting is enabled, type-1 objects that are already expired at the time of acquisition are cached (if all other conditions make the object cachable). When this setting is disabled, already expired type-1 objects become non-cachable at the time of acquisition. | disable |
| default-ttl <expiry_time> | The default expiry time for objects that do not have an expiry time set by the web server. The default expiry time is 1440 minutes (24 hours). | 1440 |
| fresh-factor <fresh_percent> | Set the fresh factor as a percentage. The default is 100, and the range is 1 to 100. For cached objects that don't have an expiry time, the web cache periodically checks the server to see if the object has expired. The higher the fresh factor the less often the checks occur. | 100 |

| Variable | Description | Default |
|--|--|---------|
| ignore-conditional {enable disable} | Enable or disable controlling the behavior of cache-control header values. HTTP 1.1 provides additional controls to the client over the behavior of caches concerning the staleness of the object. Depending on various Cache-Control headers, the FortiGate unit can be forced to consult the OCS before serving the object from the cache. For more information about the behavior of cache-control header values, see RFC 2616 . | disable |
| ignore-ie-reload {enable disable} | Some versions of Internet Explorer issue Accept / header instead of Pragma no-cache header when you select Refresh. When an Accept header has only the / value, the FortiGate unit treats it as a PNC header if it is a type-N object. When this option is enabled, the FortiGate unit ignores the PNC interpretation of the Accept: / header. | enable |
| ignore-ims {enable disable} | By default, the time specified by the if-modified-since (IMS) header in the client's conditional request is greater than the last modified time of the object in the cache, it is a strong indication that the copy in the cache is stale. If so, HTTP does a conditional GET to the Overlay Caching Scheme (OCS), based on the last modified time of the cached object. Enable <code>ignore-ims</code> to override this behavior. | disable |
| ignore-pnc {enable disable} | Typically, if a client sends an HTTP GET request with a pragma no-cache (PNC) or cache-control no-cache header, a cache must consult the OCS before serving the content. This means that the FortiGate unit always re-fetches the entire object from the OCS, even if the cached copy of the object is fresh. Because of this, PNC requests can degrade performance and increase server-side bandwidth utilization. However, if <code>ignore-pnc</code> is enabled, then the PNC header from the client request is ignored. The FortiGate unit treats the request as if the PNC header is not present at all. | disable |
| max-object-size <object_size> | Set the maximum object size to cache. The default size is 512000 kbytes (512 Mbytes). This object size determines the maximum object size to store in the web cache. All objects retrieved that are larger than the maximum size are delivered to the client but are not stored in the web cache. Range: 1 to 2 147 483 kBytes. | 512000 |
| max-ttl <expiry_time> | The maximum amount of time an object can stay in the web cache without checking to see if it has expired on the server. The default is 7200 minutes (120 hours or 5 days). | 7200 |
| min-ttl <expiry_time> | The minimum amount of time an object can stay in the web cache before checking to see if it has expired on the server. The default is 5 minutes. | 5 |

| Variable | Description | Default |
|----------------------------------|--|---------|
| neg-resp-time <response_time> | Set how long in minutes to cache negative responses. The default is 0, meaning negative responses are not cached. The content server might send a client error code (4xx HTTP response) or a server error code (5xx HTTP response) as a response to some requests. If the web cache is configured to cache these negative responses, it returns that response in subsequent requests for that page or image for the specified number of minutes. | 0 |
| reval-pnc {enable disable} | <p>The pragma-no-cache (PNC) header in a client's request can affect the efficiency of the FortiGate unit from a bandwidth gain perspective. If you do not want to completely ignore PNC in client requests (which you can do by using the ignore PNC option configuration), you can lower the impact of the PNC by enabling <code>reval-pnc</code>. When the <code>reval-pnc</code> is enabled, a client's non-conditional PNC-GET request results in a conditional GET request sent to the OCS if the object is already in the cache. This gives the OCS a chance to return the 304 Not Modified response, consuming less server-side bandwidth, because it has not been forced to return full content even though the contents have not actually changed. By default, the revalidate PNC configuration is disabled and is not affected by changes in the top-level profile. When the Substitute Get for PNC configuration is enabled, the revalidate PNC configuration has no effect.</p> <p>Most download managers make byte-range requests with a PNC header. To serve such requests from the cache, the <code>reval-pnc</code> option should be enabled along with byte-range support.</p> | disable |

webfilter

Use webfilter commands to add banned words to the banned word list, filter URLs, and configure FortiGuard-Web category filtering.

This chapter contains the following sections:

[content](#)

[content-header](#)

[fortiguard](#)

[ftgd-local-cat](#)

[ftgd-local-rating](#)

[ftgd-warning](#)

[ips-urlfilter-cache-setting](#)

[ips-urlfilter-setting](#)

[override](#)

[override-user](#)

[profile](#)

[search-engine](#)

[urlfilter](#)

content

Control web content by blocking or exempting words, phrases, or patterns.

For each pattern you can select *Block* or *Exempt*. Block, blocks access to a web page that matches with the pattern. Exempt allows access to the web page even if other entries in the list that would block access to the page.

For a page, each time a block match is found values assigned to the pattern are totalled. If a user-defined threshold value is exceeded, the web page is blocked.

Use this command to add or edit and configure options for the Web content filter list. Patterns words can be one word or a text string up to 80 characters long. The maximum number of patterns in the list is 5000.

When a single word is entered, the FortiGate unit checks Web pages for that word. Add phrases by enclosing the phrase in 'single quotes'. When a phrase is entered, the FortiGate unit checks Web pages for any word in the phrase. Add exact phrases by enclosing the phrases in "quotation marks". If the phrase is enclosed in quotation marks, the FortiGate checks Web pages for the exact phrase.

Create patterns using wildcards or Perl regular expressions.



Perl regular expression patterns are case sensitive for Web Content Filtering. To make a word or phrase case insensitive, use the regular expression `/i`. For example, `/bad language/i` blocks all instances of `bad language` regardless of case. Wildcard patterns are not case sensitive.

Syntax

```
config webfilter content
  edit <entry_number>
    set name <list_str>
    set comment <comment_str>
    config entries
      edit <content_str>
        set action {block | exempt}
        set lang {cyrillic | french | japanese | korean | simch
                | spanish | thai | trach | western}
        set pattern-type {regexp | wildcard}
        set score <score_int>
        set status {enable | disable}
      end
    end
  end
```

| Variable | Description | Default |
|--------------------------|---|---------|
| edit <entry_number> | A unique number to identify the banned word list. | |
| name <list_str> | The name of the banned word list. | |
| comment <comment_str> | The comment attached to the banned word list. | |

| Variable | Description | Default |
|---|--|----------|
| edit <content_str> | Enter the content to match. Note: multibyte characters (such as those used in Chinese, Japanese, or Korean) should be entered as character codes (e.g., &0026032;&0032862;) to ensure that the banned word is readable in the logs. | |
| action {block exempt} | Select one of: block If the pattern matches, the Score is added to the total for the web page. The page is blocked if the total score of the web page exceeds the web content block threshold defined in the web filter profile. Exempt If the pattern matches, the web page will not be blocked even if there are matching Block entries. | block |
| lang {cyrillic french japanese korean simch spanish thai trach western} | Enter the language character set used for the content. Choose from Cyrillic, French, Japanese, Korean, Simplified Chinese, Spanish, Thai, Traditional Chinese, or Western. | western |
| pattern-type {regex wildcard} | Set the pattern type for the content. Choose from <code>regex</code> or <code>wildcard</code> . Create patterns for banned words using Perl regular expressions or wildcards. | wildcard |
| score <score_int> | A numerical weighting applied to the content. The score values of all the matching words appearing on a web page are added, and if the total is greater than the <code>webwordthreshold</code> value set in the web filter profile, the page is processed according to whether the <code>bannedword</code> option is set with the <code>http</code> command in the web filter profile. The score for banned content is counted once even if it appears multiple times on the web page. | 10 |
| status {enable disable} | Enable or disable the content entry. | disable |

content-header

Use this example to filter web content according to the MIME content header. You can use this feature to broadly block content by type. But it is also useful to exempt audio and video streaming files from antivirus scanning. Scanning these file types can be problematic.

The content header list is available in the CLI only.

Syntax

```
config webfilter content-header
  edit <entry_number>
    set name <list_name>
    set comment <comment_str>
  config entries
    edit <regex>
      set action {allow | block | exempt}
      set category <fortiguard_category>
    end
  end
end
```

| Variable | Description | Default |
|-----------------------------------|--|---------|
| edit <entry_number> | A unique number to identify the content header list. | |
| name <list_name> | The name of the content header list. | |
| comment <comment_str> | The comment attached to the content header list. | |
| edit <regex> | Enter a regular expression to match the content header. For example, <code>.*image.*</code> matches image content types. | |
| action {allow block exempt} | Select one of: allow — permit matching content. block — if the pattern matches, the content is blocked. exempt — if the pattern matches, the content is exempted from antivirus scanning. | block |
| category <fortiguard_category> | Enter the FortiGuard category (or categories) to match. To view a list of categories, enter <code>set category ?</code> | |

fortiguard

Use this command to enable Web filtering by specific categories using FortiGuard-Web URL filtering.

Syntax

```
config webfilter fortiguard
    set cache-mem-percent <percent_int>
    set cache-mode {ttl | db-ver}
    set cache-prefix-match {enable | disable}
    set close-ports {enable | disable}
    set ovr-auth-cert <str>
    set ovr-auth-hostname <str>
    set ovr-auth-https {enable | disable}
    set ovr-auth-port-http <port_int>
    set ovr-auth-port-https <port_int>
    set reports-status {enable | disable}
    set request-packet-size-limit <bytes_int>
end
```

| Variable | Description | Default |
|--|--|-------------------|
| cache-mem-percent <percent_int> | Change the maximum percentage of memory the cache will use in db-ver mode. Enter a value from 1 to 15 percent. | 2 |
| cache-mode {ttl db-ver} | Change the cache entry expiration mode. Choices are ttl or db-ver. Using ttl, cache entries are deleted after a number of seconds determined by the cache-ttl setting, or until newer cache entries force the removal of older ones. When set to db-ver, cache entries are kept until the FortiGuard database changes, or until newer cache entries force the removal of older ones. | ttl |
| cache-prefix-match {enable disable} | Enable and disable prefix matching. If enabled the FortiGate unit attempts to match a packet against the rules in a prefix list starting at the top of the list. For information on prefix lists see “prefix-list, prefix-list6” on page 421 . | enable |
| close-ports {enable disable} | Enable to close ports used for HTTP/HTTPS authentication and disable user overrides. | disable |
| ovrd-auth-cert <str> | Enter a certificate name to use for FortiGuard Web Filter HTTPS override authentication. | Fortinet_Firmware |
| ovrd-auth-hostname <str> | Enter a host name to use for FortiGuard Web Filter HTTPS override authentication. | No default. |
| ovrd-auth-https {enable disable} | Enable to use HTTPS for override authentication. | enable |
| ovrd-auth-port-http <port_int> | The port to use for FortiGuard Web Filter HTTP override authentication. | 8008 |

| Variable | Description | Default |
|--|---|---------|
| ovrd-auth-port-https <port_int> | The port to use for FortiGuard Web filtering HTTPS override authentication. | 8010 |
| reports-status {enable disable} | Enable or disable FortiGuard Web Filter reports. This feature is available only on FortiGate units with an internal hard disk. | disable |
| request-packet-size-limit <bytes_int> | In some cases, FortiGuard request packets may be dropped due to IP fragmentation. You can set the maximum packet size. Range 576 to 10 000 bytes. Use 0 for the default size, 1100 bytes. | 0 |

ftgd-local-cat

Use this command to add local categories to the global URL category list. The categories defined here appear in the global URL category list when configuring a web filter profile. Users can rate URLs based on the local categories.

Syntax

```
config webfilter ftgd-local-cat
  edit <local_cat_str>
    set id <id_int>
  end
```

| Variable | Description | Default |
|-----------------|--|---------|
| <local_cat_str> | The description of the local category. | |
| id <id_int> | The local category unique ID number. | 140 |

ftgd-local-rating

Use this command to rate URLs using local categories.

Users can create user-defined categories then specify the URLs that belong to the category. This allows users to block groups of web sites on a per profile basis. The ratings are included in the global URL list with associated categories and compared in the same way the URL block list is processed.

The user can also specify whether the local rating is used in conjunction with the FortiGuard rating or is used as an override.

Syntax

```
config webfilter ftgd-local-rating
  edit <url_str>
    set rating [[<category_int>] [group_str]...]
    set status {enable | disable}
  end
```

| Variable | Description | Default |
|--|---|---------|
| <url_str> | The URL being rated. | |
| rating [[<category_int>] [group_str]...] | Set categories and/or groups. To remove items from the rating, use the unset command. Enter '?' to print a list of category and group codes with descriptions. | |
| status {enable disable} | Enable or disable the local rating. | enable |

ftgd-warning

Use this command to view FortiGuard-Web filter warnings.

When a user attempts to access a web site within a category that is configured with the warning action, the user will receive a warning which they have to acknowledge before continuing. You can view all active warnings with the `get webfilter override` command.



Although the full selection of set commands are offered, you cannot change any of the override entries. The FortiGate unit will return an error when you enter `next` or `end`.

Syntax

```
config webfilter override
  edit <override_int>
    set expires <yyyy/mm/dd hh:mm:ss>
    set initiator <user_name>
    set ip <ipv4>
    set ip6 <ipv6>
    set new-profile <profile_str>
    set old-profile <profile_str>
    set scope {user | user-group | ip | ip6}
    set status {enable | disable}
    set user <user_str>
    set user-group <user_group_str>
  end
get webfilter override <override_int>
```

| Variable | Description | Default |
|--------------------------------------|--|---|
| <override_int> | The unique ID number of the override. | |
| expires <yyyy/mm/dd hh:mm:ss> | The date and time the override expires. For example, the command to configure an expiry time of 6:45 p.m. on May 22, 2009 would be formatted this way: set expires 2010/05/22 18:45:00 | 15 minutes after the override is created. |
| initiator <user_name> | The user who initiated the override rule. This field is get-only. | |
| ip <ipv4> | When the scope is ip, enter the IP address for which the override rule applies. | 0.0.0.0 |
| ip6 <ipv6> | When the scope is ip6, enter the IP address for which the override rule applies. | :: |
| new-profile <profile_str> | Specify the new web-filter profile to apply the override. | null |
| old-profile <profile_str> | Specify the web-filter profile for which the override applies. | null |
| scope {user user-group ip ip6} | The scope of the override rule. | user |

| Variable | Description | Default |
|--------------------------------|---|---------|
| status {enable disable} | Enable or disable the override rule. | disable |
| user <user_str> | When the scope is <code>user</code> , the user for which the override rule applies. | |
| user-group <user_group_str> | When the scope is <code>user-group</code> , enter the user group for which the override rule applies. | |

ips-urlfilter-cache-setting

Use this command to configure the global DNS settings for flow-based URL filtering in conjunction with a border gateway. See also the [webfilter ips-urlfilter-cache-setting](#) command.

Syntax

```
config webfilter ips-urlfilter-cache-setting
  set dns-retry-interval <seconds_int>
  set extended-ttl <seconds_int>
end
```

| Variable | Description | Default |
|-------------------------------------|--|---------|
| dns-retry-interval <seconds_int> | Set the DNS retry interval. Refresh DNS faster than TTL to capture multiple IPs for hosts. Range 0 to 2 147 483. 0 means use DNS server's TTL value. | 0 |
| extended-ttl <seconds_int> | Extend the TTL beyond that of the DNS server. Range 0 to 2 147 483. | 0 |

ips-urlfilter-setting

Use this command to set up url filtering (flow-based) in conjunction with a border gateway router.

Syntax

```
config webfilter ips-urlfilter-setting
  set device <intf_name>
  set distance <dist_int>
  set gateway <ip_addr>
end
```

| Variable | Description | Default |
|------------------------|--|-------------|
| device <intf_name> | Select the interface that connects to the border router. | No default. |
| distance <dist_int> | Set the administrative distance. Range 1 to 255. | 1 |
| gateway <ip_addr> | Enter the IP address of the border router. | 0.0.0.0 |

override

Use this command to configure FortiGuard-Web filter administrative overrides.

The administrative overrides are backed up with the main configuration and managed by the FortiManager system. The administrative overrides are not cleaned up when they expire and you can reuse these override entries by extending their expiry dates.

Syntax

```
config webfilter override
  get webfilter override <override_int>
  edit <override_int>
    set expires <yyyy/mm/dd hh:mm:ss>
    set initiator <user_name>
    set ip <ipv4>
    set ip6 <ipv6>
    set new-profile <profile_str>
    set old-profile <profile_str>
    set scope {user | user-group | ip | ip6}
    set status {enable | disable}
    set user <user_str>
    set user-group <user_group_str>
  end
```

| Variable | Description | Default |
|--------------------------------------|--|---|
| <override_int> | The unique ID number of the override. | |
| expires <yyyy/mm/dd hh:mm:ss> | The date and time the override expires. For example, the command to configure an expiry time of 6:45 p.m. on May 22, 2015 would be formatted this way: set expires 2015/05/22 18:45:00 | 15 minutes after the override is created. |
| initiator <user_name> | The user who initiated the override rule. This field is get-only. | |
| ip <ipv4> | When the scope is ip, enter the IP address for which the override rule applies. | 0.0.0.0 |
| ip6 <ipv6> | When the scope is ip6, enter the IP address for which the override rule applies. | :: |
| new-profile <profile_str> | Specify the new web-filter profile to apply the override. | null |
| old-profile <profile_str> | Specify the web-filter profile for which the override applies. | null |
| scope {user user-group ip ip6} | The scope of the override rule. | user |
| status {enable disable} | Enable or disable the override rule. | disable |
| user <user_str> | When the scope is user, the user for which the override rule applies. | |
| user-group <user_group_str> | When the scope is user-group, enter the user group for which the override rule applies. | |

override-user

Use this command to configure FortiGuard-Web filter user overrides.

When a user attempts to access a blocked site, if override is enabled, a link appears on the block page directing the user to an authentication form. The user must provide a correct user name and password or the web site remains blocked. Authentication is based on user groups and can be performed for local, RADIUS, and LDAP users.

Administrators can only view and delete the user overrides entries.

Syntax

```
config webfilter override-user
  edit <override_int>
    set expires <yyyy/mm/dd hh:mm:ss>
    set initiator <user_name>
    set ip <ipv4>
    set ip6 <ipv6>
    set new-profile <profile_str>
    set old-profile <profile_str>
    set scope {user | user-group | ip | ip6}
    set status {enable | disable}
    set user <user_str>
    set user-group <user_group_str>
  end
get webfilter override-user <override_int>
```

| Variable | Description | Default |
|--------------------------------------|--|---|
| <override_int> | The unique ID number of the override. | |
| expires <yyyy/mm/dd hh:mm:ss> | The date and time the override expires. For example, the command to configure an expiry time of 6:45 p.m. on May 22, 2009 would be formatted this way: set expires 2010/05/22 18:45:00 | 15 minutes after the override is created. |
| initiator <user_name> | The user who initiated the override rule. This field is get-only. | |
| ip <ipv4> | When the scope is IP, enter the IP address for which the override rule applies. | 0.0.0.0 |
| ip6 <ipv6> | When the scope is ip6, enter the IP address for which the override rule applies. | :: |
| new-profile <profile_str> | Specify the new web-filter profile to apply the override. | null |
| old-profile <profile_str> | Specify the web-filter profile for which the override applies. | null |
| scope {user user-group ip ip6} | The scope of the override rule. | user |
| status {enable disable} | Enable or disable the override rule. | disable |

| Variable | Description | Default |
|--------------------------------|---|---------|
| user <user_str> | When the scope is <code>user</code> , the user for which the override rule applies. | |
| user-group <user_group_str> | When the scope is <code>user-group</code> , the user group for which the override rule applies. | |

profile

Use this command to configure UTM web filtering profiles for firewall policies. Web filtering profiles configure how web filtering and FortiGuard Web Filtering is applied to sessions accepted by a firewall policy that includes the web filter profile.

Syntax

```
config webfilter profile
  edit <name_str>
    set comment <comment_str>
    set extended-utm-log {enable | disable}
    set flow-based {enable | disable}
    set https-replacemsg {enable | disable}
    set log-all-urls {enable | disable}
    set options {activexfilter | block-invalid-url | cookiefilter
      | https-scan | intrinsic | javafilter | js | jscript
      | per-user-bwl | rangeblock | unknown | vbs | wf-cookie
      | wf-referer}
    set ovrd-perm [bannedword-override contenttype-check-override
      fortiguard-wf-override urlfilter-override]
    set post-action {normal | comfort | block}
    set web-content-log {enable | disable}
    set web-filter-activex-log {enable | disable}
    set web-filter-command-block-log {enable | disable}
    set web-filter-cookie-log {enable | disable}
    set web-filter-cookie-removal-log {enable | disable}
    set web-filter-applet-log {enable | disable}
    set web-filter-js-log {enable | disable}
    set web-filter-jscript-log {enable | disable}
    set web-filter-vbs-log {enable | disable}
    set web-filter-unknown-log {enable | disable}
    set web-filter-referer-log {enable | disable}
    set web-ftgd-err-log {enable | disable}
    set web-ftgd-quota-usage {enable | disable}
    set web-invalid-domain-log {enable | disable}
    set web-url-log {enable | disable}
  config ftgd-wf
    set options {connect-request-bypass | error-allow
      | ftgd-disable | http-err-detail | rate-image-urls
      | rate-server-ip | redir-block | strict-blocking}
    set category-override <category_str>
    set exempt-quota {all | <category_str>}
    set exempt-ssl {all | <category_str>}
```

```

Variables for config filters
edit <id_str>
    set action {authenticate | block | monitor | warning}
    set auth-usr-group [group1 ...groupn]
    set category {category_int group_str}
    set log {enable | disable}
    set warn-duration <dur_string>
end
config quota
edit <id>
    set category <id>
    set duration <dur_str>
    set type {time | traffic}
    set unit {B | GB | KB | MB}
    set value <int>
end
end
config override
set ovr-dur <###d##h##m>
set ovr-dur-mode {ask | constant}
set ovr-scope {ask | ip | user | user-group}
set ovr-user-group <groupname_str> [<groupname_str>...]
set profile <web_profile>
set profile-attribute <attribute_str>
set profile-type {list | radius}
end
config web
set bword-threshold <threshold_int>
set bword-table <filter_list_name>
set urlfilter-table <url_list_name>
set content-header-list <list_number>
set keyword-match <pattern_str>
set log-search {enable | disable}
set safe-search {url | header}
set urlfilter-table <url_list_name>
set youtube-edu-filter-id <accountid_int>
end
end

```

| Variable | Description | Default |
|--|--|---------|
| <name_str> | Enter the name of the web filtering profile. | |
| comment <comment_str> | Optionally enter a description of up to 63 characters of the web filter profile. | |
| extended-utm-log {enable disable} | Enable or disable detailed UTM log messages. | disable |
| flow-based {enable disable} | Enable or disable flow-based web filtering. | disable |
| https-replacemsg {enable disable} | Enable replacement message display for non-deep SSL inspection. | enable |

| Variable | Description | Default |
|---|---|---------|
| log-all-urls {enable disable} | Enable to log all URLs, even if FortiGuard is not enabled. extended-utm-log must be enabled. | disable |
| options {activexfilter block-invalid-url cookiefilter https-scan intrinsic javafilter js jscript per-user-bwl rangeblock unknown vbs wf-cookie wf-referer} | <p>Select one or more options apply to web filtering. To select more than one, enter the option names separated by a space. Some options are only available for some protocols.</p> <p>activexfilter — block ActiveX plugins.</p> <p>block-invalid-url — block web pages with an invalid domain name.</p> <p>cookiefilter — block cookies.</p> <p>https-scan — enable encrypted content scanning for HTTPS traffic. This option is available only on FortiGate units that support encrypted content scanning.</p> <p>intrinsic — block intrinsic scripts.</p> <p>javafilter — block Java applets.</p> <p>js — block JavaScript applets.</p> <p>jscript — block JavaScript applets.</p> <p>per-user-bwl — per-user black/white list. This must also be enabled in system global.</p> <p>rangeblock — block downloading parts of a file that have already been partially downloaded. Selecting this option prevents the unintentional download of virus files hidden in fragmented files. Note that some types of files, such as PDF, fragment files to increase download speed and enabling this option can cause download interruptions. Enabling this option may break certain applications that use the Range Header in the HTTP protocol, such as YUM, a Linux update manager.</p> <p>unknown — block unknown scripts.</p> <p>vbs — block VB scripts.</p> <p>wf-cookie — block the contents of the HTTP header “Cookie”.</p> <p>wf-referer — block the contents of the HTTP header “Referer”.</p> <p>Separate multiple options with a space. To remove an option from the list or add an option to the list, retype the list with the option removed or added.</p> | |

| Variable | Description | Default |
|---|--|----------|
| ovrd-perm [bannedword-override contenttype-check-overri de fortiguard-wf-override urlfilter-override] | Override permit options: bannedword-override — content block contenttype-check-override — filter based on content-type header override fortiguard-wf-override — FortiGuard Web Filter block override urlfilter-override — web url filter override | null |
| post-action {normal comfort block} | Select the action to take with HTTP POST traffic. This option is available for HTTPS normal — do not affect HTTP POST traffic. comfort — use the comfort-interval and comfort-amount http options of the “firewall profile-protocol-options” on page 190 to send comfort bytes to the server in case the client connection is too slow. Select this option to prevent a server timeout when scanning or other filtering tool is turned on. block — block HTTP POST requests. When the post request is blocked the FortiGate unit sends the http-post-block replacement message to the user’s web browser. | normal |
| web-content-log {enable disable} | Enable or disable logging for web content blocking. | enable |
| web-filter-activex-log {enable disable} | Enable or disable logging for activex script web filtering. | enable |
| web-filter-command-block-log {enable disable} | Enable or disable logging of web filter command block messages. | enable |
| web-filter-cookie-log {enable disable} | Enable or disable logging for cookie script web filtering. | enable |
| web-filter-cookie-removal-log {enable disable} | Enable or disable logging for web filter cookie blocking. | enable |
| web-filter-applet-log {enable disable} | Enable or disable logging for applet script web filtering. | enable |
| web-filter-js-log {enable disable} | Enable or disable logging for web script filtering on javascripts. | enable |
| web-filter-jscript-log {enable disable} | Enable or disable logging for web script filtering on JScripts. | enable |
| web-filter-sdns-action {redirect block} | Select the action for FortiGuard DNS-based webfiltering: redirect user to a captive portal or block the connection. | redirect |
| web-filter-sdns-portal <portal_ip> | Enter the captive portal IP address used for users redirected by FortiGuard DNS-based webfiltering. | 0.0.0.0 |
| web-filter-vbs-log {enable disable} | Enable or disable logging for web script filtering on VBS scripts. | enable |
| web-filter-unknown-log {enable disable} | Enable or disable logging for web script filtering on unknown scripts. | enable |

| Variable | Description | Default |
|--|---|---------|
| web-filter-referer-log {enable disable} | Enable or disable logging for webfilter referer block. | enable |
| web-ftgd-err-log {enable disable} | Enable or disable logging for FortiGuard Web Filtering rating errors. | enable |
| web-ftgd-quota-usage {enable disable} | Enable or disable logging for FortiGuard Web Filtering daily quota usage. | enable |
| web-invalid-domain-log {enable disable} | Enable or disable logging for web filtering of invalid domain names. | enable |
| web-url-log {enable disable} | Enable or disable logging for web URL filtering. | enable |

config ftgd-wf

Configure FortiGuard Web Filtering options.

For the `enable`, `disable`, `allow`, `deny`, `log`, `ovrd`, `ftgd-wf-ssl-exempt` options, to view a list of available category codes with their descriptions, enter `get`, then find entries such as `g01 Potentially Liable`, `1 Drug Abuse`, and `c06 Spam URL`. Separate multiple codes with a space. To delete entries, use the `unset` command to delete the entire list.

| Variable | Description | Default |
|--|--|---------|
| category-override <category_str> | Enable local categories to take precedence over FortiGuard Web Filtering categories. Enter category numbers or group numbers separated by spaces. | null |
| exempt-quota {all <category_str>} | Do not stop quota for these categories. | |
| exempt-ssl {all <category_str>} | Enter categories to exempt from SSL inspection. | |
| options {connect-request-bypass error-allow ftgd-disable http-err-detail rate-image-urls rate-server-ip redir-block strict-blocking} | <p>Select options for FortiGuard web filtering, separating multiple options with a space.</p> <p><code>connect-request-bypass</code> — (http only) bypass FortiGuard Web Filtering for HTTP sessions to the same address as bypassed HTTPS connections.</p> <p><code>error-allow</code> — allow web pages with a rating error to pass through.</p> <p><code>ftgd-disable</code> — disable FortiGuard.</p> <p><code>http-err-detail</code> — display a replacement message for 4xx and 5xx HTTP errors. If error pages are allowed, malicious or objectionable sites could use these common error pages to circumvent web category blocking. This option does not apply to HTTPS.</p> <p><code>rate-image-urls</code> — rate images by URL. Blocked images are replaced with blanks. This option does not apply to HTTPS.</p> <p><code>rate-server-ip</code> — send both the URL and the IP address of the requested site for checking, providing additional security against attempts to bypass the FortiGuard system.</p> | |

| Variable | Description | Default |
|--|---|-------------|
| | <p><code>redir-block</code> — block HTTP redirects. Many web sites use HTTP redirects legitimately; however, in some cases, redirects may be designed specifically to circumvent web filtering, as the initial web page could have a different rating than the destination web page of the redirect.</p> <p><code>strict-blocking</code> — block any web pages if any classification or category matches the rating. This option does not apply to HTTPS.</p> <p>To remove an option from the list or add an option to the list, retype the list with the option removed or added.</p> <p>These options take effect only if FortiGuard web filtering is enabled for the protocol.</p> | |
| Variables for config filters | | |
| <code><id_str></code> | Enter the ID number of the filter. Enter a new number to create a new filter. Enter an existing number to edit a filter. | |
| <code>action {authenticate block monitor warning}</code> | <p>Enter the action to take for matches.</p> <p><code>authenticate</code> permits authenticated users to load the web page.</p> <p><code>block</code> prevents the user from loading the web page.</p> <p><code>monitor</code> permits the user to load the web page but logs the action.</p> <p><code>warning</code> requires that the user acknowledge a warning before they can proceed.</p> | block |
| <code>auth-usr-group [group1 ...groupn]</code> | <p>Enter the user groups who are permitted to authenticate.</p> <p>This is available if <code>action</code> is <code>authenticate</code>.</p> | No default. |
| <code>category {category_int group_str}</code> | Enter the categories and groups the filter will examine. You can specify multiple categories and groups by separating them with a space character. | No default. |
| <code>log {enable disable}</code> | Enable or disable logging for this filter. | enable |
| <code>warn-duration <dur_string></code> | <p>Set duration (<i>nnhnnmmns</i>, 23h59m59s for example) of warning.</p> <p>This is available when <code>action</code> is <code>warning</code> or <code>authenticated</code>.</p> | 5m |

config override

Configure web filtering overrides.

| Variable | Description | Default |
|--|---|-------------------|
| ovrd-dur <###d##h##m> | Enter the FortiGuard Web Filtering override duration in days, hours, and minutes in any combination. For example, 34d, 12h, 20m, 34d23m, 200d12h45m. The maximum is 364d23h59m. | 15m |
| ovrd-dur-mode {ask constant} | Enter the FortiGuard Web Filtering duration type, one of: constant — as specified in <code>ftgd-wf-ovrd-dur</code> ask — ask for duration when initiating override. <code>ftgd-wf-ovrd-dur</code> is the maximum | constant |
| ovrd-scope {ask ip user user-group} | Enter the scope of the Web Filtering override, one of: ask — ask for scope when initiating an override. ip — override for the initiating IP — user — override for the user user-group — override for a user group | user |
| ovrd-user-group <groupname_str> [<groupname_str>...] | Enter the names of user groups that can be used for FortiGuard Web Filter overrides. Separate multiple names with spaces. | null |
| profile <web_profile> | Enter the web profile name. | |
| profile-attribute <attribute_str> | Enter the name of the profile attribute to retrieve from the RADIUS server. Available when <code>profile-type</code> is <code>radius</code> . | Login-LAT-service |
| profile-type {list radius} | Enter <code>list</code> if the override profile chosen from a list. Enter <code>radius</code> if the override profile is determined by a RADIUS server. | |

config quota

Configure FortiGuard quotas.

| Variable | Description | Default |
|----------------------------|--|-------------|
| edit <id> | Enter an ID for the quota. | No default. |
| category <id> | Set the category. The category must have action of <code>monitor</code> and must not be in <code>exempt-ssl</code> list. | No default. |
| duration <dur_str> | Set the duration (<i>nnhnnmnn</i> s). | 5m |
| | | |
| type {time traffic} | Set the quota type: time-based or traffic-based. | time |
| unit {B GB KB MB} | Set the unit for traffic based quota. | MB |
| value <int> | Set the quota numeric value. | 0 |

config web

Specify the web content filtering the web URL filtering lists to use with the web filtering profile and set other configuration setting such as the web content filter threshold.

| Variable | Description | Default |
|--|--|-------------|
| bword-threshold <threshold_int> | If the combined scores of the web content filter patterns appearing in a web page exceed the threshold value, the web page is blocked. The rang is 0-2147483647. | 10 |
| bword-table <filter_list_name> | Select the name of the web content filter list to use with the web filtering profile. | |
| content-header-list <list_number> | Select the content header list. | 0 |
| keyword-match <pattern_str> | Search keywords to log. | |
| log-search {enable disable} | Enable or disable logging all search phrases. | disable |
| safe-search {url header} | Select whether safe search is based on the request URL or header. | Null |
| urlfilter-table <url_list_name> | Select the name of the URL filter list to use with the web filtering profile. | No default. |
| youtube-edu-filter-id <accountid_int> | Enter the account ID for YouTube Education Filter. Available when <code>safe-search</code> is header. | No default. |

search-engine

Use this command to configure search engine definitions. Definitions for well-known search engines are included by default.

Syntax

```
config webfilter search-engine
  edit <site_name>
    set hostname <url_regex>
    set query <str>
    set safesearch {disable | header | url}
    set safesearch-str
    set url <url_str>
  end
```

| Variable | Description | Default |
|--|--|-------------|
| <site_name> | Enter the name of the search engine. | No default. |
| hostname <url_regex> | Enter the regular expression to match the hostname portion of the search URL. For example, <code>.*\.google\..*</code> for Google. | No default. |
| query <str> | Enter the code used to prefix a query. | No default. |
| safesearch {disable header url} | Select how to request safe search on this site. disable — site does not support safe search header — selected by search header, e.g. youtube.edu url — selected with a parameter in the URL | disable |
| safesearch-str | Enter the safe search parameter used in the URL. Example: <code>&safe=on</code> This is available if safesearch is url. | No default. |
| url <url_str> | Enter the regular expression to match the search URL. For example <code>^\/((custom search images videosearch webhp)\?)</code> | No default. |

urlfilter

Use this command to control access to specific URLs by adding them to the URL filter list. The FortiGate unit exempts or blocks Web pages matching any specified URLs and displays a replacement message instead.

Configure the FortiGate unit to allow, block, or exempt all pages on a website by adding the top-level URL or IP address and setting the action to allow, block, or exempt.

Block individual pages on a website by including the full path and filename of the web page to block. Type a top-level URL or IP address to block access to all pages on a website. For example, `www.example.com` or `172.16.144.155` blocks access to all pages at this website.

Type a top-level URL followed by the path and filename to block access to a single page on a website. For example, `www.example.com/news.html` or `172.16.144.155/news.html` blocks the news page on this website.

To block all pages with a URL that ends with `example.com`, add `example.com` to the block list. For example, adding `example.com` blocks access to `www.example.com`, `mail.example.com`, `www.finance.example.com`, and so on.

Use this command to exempt or block all URLs matching patterns created using text and regular expressions (or wildcard characters). For example, `example.*` matches `example.com`, `example.org`, `example.net` and so on. The FortiGate unit exempts or blocks Web pages that match any configured pattern and displays a replacement message instead.

Syntax

```
config webfilter urlfilter
  edit <list_int>
    set name <list_str>
    set comment <comment_str>
    set one-arm-ips-urlfilter {enable | disable}
    config entries
      edit <url_str>
        set action {allow | block | exempt | monitor}
        set exempt {all activex-java-cookie av dlp fortiguard pass
          range-block web-content}
        set status {enable | disable}
        set type {simple | regex | wildcard}
      end
    end
  end
```

| Variable | Description | Default |
|---|--|---------|
| <list_int> | A unique number to identify the URL filter list. | |
| name <list_str> | The name of the URL filter list. | |
| comment <comment_str> | The comment attached to the URL filter list. | |
| one-arm-ips-urlfilter {enable disable} | Enable or disable IPS URL filter. | disable |
| <url_str> | The URL to added to the list. | |

| Variable | Description | Default |
|---|--|--|
| action {allow block exempt monitor} | <p>The action to take for matches.</p> <p>An <code>allow</code> match exits the URL filter list and checks the other web filters.</p> <p>A <code>block</code> match blocks the URL and no further checking will be done.</p> <p>An <code>exempt</code> match stops all further checking including AV scanning for the current HTTP session, which can affect multiple URLs.</p> <p>A <code>monitor</code> match passes the URL and generates a log message. The request is still subject to other UTM inspections.</p> | exempt |
| exempt {all activex-java-cookie av dlp fortiguard pass range-block web-content} | <p>Enter the types of scanning to skip for the exempt URLs:</p> <p><code>all</code> — Exempt from all.</p> <p><code>activex-java-cookie</code> — activeX, Java, and cookies</p> <p><code>av</code> — antivirus scanning</p> <p><code>dlp</code> — DLP scanning</p> <p><code>fortiguard</code> — FortiGuard web filtering</p> <p><code>pass</code> — pass single connection from all.</p> <p><code>range-block</code> — do not allow range-block</p> <p><code>web-content</code> — web filter content matching</p> | activex-java-cookie all av dlp fortiguard range-block web-content |
| status {enable disable} | The status of the filter. | enable |
| type {simple regex wildcard} | The type of URL filter: simple, regular expression, or wildcard. | simple |

web-proxy

Use these commands to configure the FortiGate web proxy. You can use the FortiGate web proxy and interface settings to enable explicit HTTP and HTTPS proxying on one or more interfaces. When enabled, the FortiGate unit becomes a web proxy server. All HTTP and HTTPS session received by interfaces with explicit web proxy enabled are intercepted by the explicit web proxy relayed to their destinations.

To use the explicit proxy, users must add the IP address of a FortiGate interface and the explicit proxy port number to the proxy configuration settings of their web browsers.

On FortiGate units that support WAN optimization, you can also enable web caching for the explicit proxy.

[explicit](#)

[forward-server](#)

[forward-server-group](#)

[global](#)

[url-match](#)

explicit

Use this command to enable the explicit web proxy, and configure the TCP port used by the explicit proxy.

Syntax

```
config web-proxy explicit
  set status {enable | disable}
  set ftp-over-http {enable | disable}
  set socks {enable | disable}
  set http-incoming-port <http_port_int>
  set https-incoming-port <https_port_int>
  set ftp-incoming-port <ftp_port_int>
  set socks-incoming-port <socks_port_int>
  set incoming-ip <incoming_interface_ipv4>
  set incoming-ip6 <incoming_interface_ipv6>
  set ipv6-status {enable | disable}
  set outgoing-ip <outgoing_interface_ipv4>
    [<outgoing_interface_ipv4> ... <outgoing_interface_ipv4>]
  set outgoing-ip6 <outgoing_interface_ipv6>
    [<outgoing_interface_ipv6> ... <outgoing_interface_ipv6>]
  set unknown-http-version {best-effort | reject}
  set realm <realm_str>
  set sec-default-action {accept | deny}
  set pac-file-server-status {enable | disable}
  set pac-file-server-port <pac_port_int>
  set pac-file-name <pac_file_str>
  set pac-file-data <pac_file_str>
  set pac-file-url <url_str>
  set ssl-algorithm {low | medium | high}
end
```

| Variable | Description | Default |
|------------------------------------|---|---------|
| status {enable disable} | Enable the explicit web proxy for HTTP and HTTPS sessions. | disable |
| ftp-over-http {enable disable} | Configure the explicit proxy to proxy FTP sessions sent from a web browser. The explicit proxy only supports FTP with a web browser and not with a standalone FTP client. | disable |
| socks {enable disable} | Configure the explicit proxy to proxy SOCKS sessions sent from a web browser. For information about SOCKS, see RFC 1928 . The explicit web proxy supports SOCKS 4 and 5. | disable |
| http-incoming-port <http_port_int> | Enter the port number that HTTP traffic from client web browsers use to connect to the explicit proxy. The range is 0 to 65535. Explicit proxy users must configure their web browser's HTTP proxy settings to use this port. | 8080 |

| Variable | Description | Default |
|---|--|---------|
| https-incoming-port <https_port_int> | Enter the port number that HTTPS traffic from client web browsers use to connect to the explicit proxy. The range is 0 to 65535. Explicit proxy users must configure their web browser's HTTPS proxy settings to use this port. The default value of 0 means use the same port as HTTP. | 0 |
| ftp-incoming-port <ftp_port_int> | Enter the port number that FTP traffic from client web browsers use to connect to the explicit proxy. The range is 0 to 65535. Explicit proxy users must configure their web browser's FTP proxy settings to use this port. The default value of 0 means use the same port as HTTP. | 0 |
| socks-incoming-port <socks_port_int> | Enter the port number that SOCKS traffic from client web browsers use to connect to the explicit proxy. The range is 0 to 65535. Explicit proxy users must configure their web browser's SOCKS proxy settings to use this port. The default value of 0 means use the same port as HTTP. | 0 |
| incoming-ip <incoming_interface_ipv4> | Enter the IP address of a FortiGate unit interface that should accept sessions for the explicit web proxy. Use this command to restrict the explicit web proxy to only accepting sessions from one FortiGate interface. The destination IP address of explicit web proxy sessions should match this IP address. This field is not available in Transparent mode. | 0.0.0.0 |
| incoming-ip6 <incoming_interface_ipv6> | Enter the IPv6 address of a FortiGate unit interface that should accept sessions for the explicit web proxy. Use this command to restrict the explicit web proxy to only accepting sessions from one FortiGate interface. This is available when <code>ipv6-status</code> is enable. | ::0 |
| ipv6-status {enable disable} | Enable or disable IPv6 web-proxy operation. | disable |
| outgoing-ip <outgoing_interface_ipv4> [<outgoing_interface_ipv4> ... <outgoing_interface_ipv4>] | Enter the IP address of a FortiGate unit interface that explicit web proxy sessions should exit the FortiGate unit from. Multiple interfaces can be specified. Use this command to restrict the explicit web proxy to only allowing sessions to exit from one FortiGate interface. This IP address becomes the source address of web proxy sessions exiting the FortiGate unit. This field is not available in Transparent mode. | 0.0.0.0 |

| Variable | Description | Default |
|---|--|---------|
| outgoing-ipv6 <outgoing_interface_ipv6> [<outgoing_interface_ipv6> ... <outgoing_interface_ipv6>] | <p>Enter the IPv6 address of a FortiGate unit interface that explicit web proxy sessions should exit the FortiGate unit from. Multiple interfaces can be specified. Use this command to restrict the explicit web proxy to only allowing sessions to exit from one FortiGate interface.</p> <p>This IP address becomes the source address of web proxy sessions exiting the FortiGate unit.</p> <p>This field is not available in Transparent mode.</p> | ::0 |
| unknown-http-version {best-effort reject} | <p>Select the action to take when the proxy server must handle an unknown HTTP version request or message. Choose from either Reject or Best Effort.</p> <p>Best Effort attempts to handle the HTTP traffic as best as it can. Reject treats unknown HTTP traffic as malformed and drops it. The Reject option is more secure.</p> | reject |
| realm <realm_str> | <p>Enter an authentication realm to identify the explicit web proxy. The realm is a text string of up to 63 characters. If the realm includes spaces enclose it in quotes. Only alphanumeric characters are permitted. FortiOS rejects the string if it contains special characters.</p> <p>When a user authenticates with the explicit proxy the HTTP authentication dialog includes the realm so you can use the realm to identify the explicit web proxy for your users.</p> | default |
| sec-default-action {accept deny} | <p>Configure the explicit web proxy to block (deny) or accept sessions if firewall policies have not been added for the explicit web proxy. To add firewall policies for the explicit web proxy add a firewall policy and set the source interface to web-proxy.</p> <p>The default setting denies access to the explicit web proxy before adding a firewall policy. If you set this option to <code>accept</code> the explicit web proxy server accepts sessions even if you haven't defined a firewall policy.</p> | deny |
| pac-file-server-status {enable disable} | <p>Enable support for proxy auto-config (PAC). With PAC support enabled you can configure a PAC file on the FortiGate unit and distribute the URL of this file to your web browser users. These users can enter this URL as an automatic proxy configuration URL and their browsers will automatically download proxy configuration settings.</p> <p>You can use PAC to provide access to multiple proxy servers and access methods as well as other features.</p> <p>To enable PAC you must edit or replace (by importing) the default PAC file installed in your FortiGate unit.</p> | disable |

| Variable | Description | Default |
|--|--|-----------|
| pac-file-server-port <pac_port_int> | Select the port that PAC traffic from client web browsers use to connect to the explicit proxy. The range is 0 to 65535. Explicit proxy users must configure their web browser's PAC proxy settings to use this port. The default value of 0 means use the same port as HTTP. | 0 |
| pac-file-name <pac_file_str> | Change the name of the PAC file. In most cases you could keep the default name. | proxy.pac |
| pac-file-data <pac_file_str> | Enter the contents of the PAC file made available from the explicit proxy server for PAC support. Enclose the PAC file text in quotes. You can also copy the contents of a PAC text file and paste the contents into the CLI using this option. Enter the command followed by two sets of quotes then place the cursor between the quotes and paste the file content. The maximum PAC file size is 8192 bytes. You can use any PAC file syntax that is supported by your users's browsers. The FortiGate unit does not parse the PAC file. | |
| pac-file-url <url_str> | Displays the PAC file URL in the format: <code>http://<interface_ip>: <PAC_port_int>/<pac_file_str></code> For example, if the interface with the explicit web proxy has IP address 172.20.120.122, the PAC port is the same as the default HTTP explicit proxy port (8080) and the PAC file name is proxy.pac the PAC file URL would be: <code>http://172.20.120.122:8080/proxy.pac</code> If the explicit web proxy is enabled on multiple interfaces there will be multiple PAC URLs. If you have configured an <code>incoming-ip</code> only one PAC file URL is listed that includes the <code>incoming-ip</code> . Distribute this URL to PAC users. You cannot use the <code>pac-file-url</code> option to edit the PAC file URL. | |
| ssl-algorithm {low medium high} | Select the strength of encryption algorithms accepted for deep scan: high: AES, 3DES low: AES, 3DES, RC4, DES medium: AES, 3DES, RC4 | medium |

forward-server

Use this command to support explicit web proxy forwarding, also called proxy chaining.

Syntax

```
config web-proxy forward-server
edit <server_name_string>
    set addr-type {fqdn | ip}
    set comment <comment_string>
    set fqdn <fqdn_string>
    set healthcheck {enable | disable}
    set ip <server_ipv4>
    set monitor <http_url>
    set port <port_integer>
    set server-down-option {block | pass}
end
```

| Variable | Description | Default |
|--------------------------------------|--|-------------|
| addr-type {fqdn ip} | Select whether proxy address is defined by domain name (fqdn) or IP address. | ip |
| comment <comment_string> | Optionally, enter a description. | No default. |
| fqdn <fqdn_string> | Enter the fully qualified domain name of the forwarding web proxy server. Available if addr-type is fqdn. | No default. |
| healthcheck {enable disable} | Enable or disable proxy server health check. Health checking attempts to connect to a web server to make sure that the remote forwarding server is operating. | disable |
| ip <server_ipv4> | Enter the IP address of the forwarding proxy server. Available if addr-type is ip. | 0.0.0.0 |
| monitor <http_url> | Enter the URL to use for health check monitoring. This would be a URL that the web proxy would attempt to connect to through the forwarding server. If the web proxy can't connect to this URL it assumes the forwarding server is down. | |
| port <port_integer> | Enter the port number that the forwarding server expects to receive HTTP sessions on. | 3128 |
| server-down-option {block pass} | Select the action to take when the forwarding proxy server is down: block — block sessions until the server comes back up pass — allow sessions to connect to their destination | block |

forward-server-group

Use this command to configure a load-balanced group of web proxy forward servers.

Syntax

```
config web-proxy forward-server-group
  edit <fwdsrvr_group_name>
    set affinity {enable | disable}
    set group-down-option {pass | block}
    set ldb-method {least-session | weighted}
  config server-list
    edit <fwd-srvr-name>
      set weight <weight_int>
    end
  end
end
```

| Variable | Description | Default |
|---|---|----------|
| affinity {enable disable} | Enable to attach source-ip's traffic to assigned forward-server until <code>forward-server-affinity-timeout</code> (see web-proxy global). | enable |
| group-down-option {pass block} | Select action to take if all forward servers are down: pass traffic through or block traffic. | block |
| ldb-method {least-session weighted} | Select the load-balancing method. | weighted |
| weight <weight_int> | Set weight of this server for load balancing. Range 1 to 100. | 10 |

global

Configure global web-proxy settings that control how the web proxy functions and handles web traffic. In most cases you should not have to change the default settings of this command. If your FortiGate unit is operating with multiple VDOMs these settings affect all VDOMs.

Syntax

```
config web-proxy global
    set add-header-client-ip {enable | disable}
    set add-header-via {enable | disable}
    set add-header-x-forwarded-for {enable | disable}
    set add-header-front-end-https {enable | disable}
    set forward-proxy-auth {enable | disable}
    set forward-server-affinity-timeout <minutes_int>
    set max-message-length <kBytes>
    set max-request-length <kBytes>
    set proxy-fqdn <fqdn>
    set strict-web-check {enable | disable}
    set tunnel-non-http {enable | disable}
    set unknown-http-version {tunnel | best-effort | reject}
end
```

| Variable | Description | Default |
|--|--|---------|
| add-header-client-ip {enable disable} | Enable to add the client IP to the header of forwarded requests | disable |
| add-header-front-end-https {enable disable} | Enable to add a front-end-https header to forwarded requests. | disable |
| add-header-via {enable disable} | Enable to add the via header to forwarded requests. | disable |
| add-header-x-forwarded-for {enable disable} | Enable to add x-forwarded-for header to forwarded requests. | disable |
| forward-proxy-auth {enable disable} | In explicit mode, enable to forward proxy authentication headers. By default proxy authentication headers are blocked by the explicit web proxy. You can set this option to enable if you need to allow proxy authentication through the explicit web proxy. This option does not apply to web proxy transparent mode, because in transparent mode, proxy authentication headers are always forwarded by the web proxy. | disable |
| forward-server-affinity-timeout <minutes_int> | The source-ip's traffic will attach to assigned forward-server until timeout. Range: 6 to 60 minutes. | 30 |
| max-message-length <kBytes> | Set the maximum length, in kBytes, of the HTTP message not including body. Range 16 to 256. | 32 |
| max-request-length <kBytes> | Set the maximum length, in kBytes, of the HTTP request line. Range 2 to 64. | 4 |

| Variable | Description | Default |
|---|--|--------------|
| proxy-fqdn <fqdn> | Set the fully qualified domain name (FQDN) for the proxy. This is the domain that clients connect to. | default.fqdn |
| strict-web-check {enable disable} | Enable to block web sites that send incorrect headers that do not conform to HTTP 1.1 as described in RFC 2616 . Disable to allow and cache websites that send incorrect headers that do not conform to the RFC. This option is disabled by default so that web sites are not blocked. You can enable this option if you want to increase security by blocking sites that do not conform. Enabling this option may block some commonly used websites. | disable |
| tunnel-non-http {enable disable} | Enable to allow non-HTTP traffic. | enable |
| unknown-http-version {tunnel best-effort reject} | Select how to handle traffic if HTTP version is unknown: tunnel — tunnel the traffic best-effort — proceed with best effort reject — reject the traffic | best-effort |

url-match

Use this command to define URLs for forward-matching or cache exemption.

Syntax

```
config web-proxy url-match
  edit <url-pattern>
    set cache-exemption {enable | disable}
    set comment <comment_str>
    set forward-server <name_str>
    set status {enable | disable}
    set url-pattern <pattern_str>
  end
```

| Variable | Description | Default |
|------------------------------------|--|---------|
| cache-exemption {enable disable} | Enable to set a cache exemption list. User defined URLs in the list will be exempted from caching. | disable |
| comment <comment_str> | Optionally enter a comment. | |
| forward-server <name_str> | Enter the forward server name. | |
| status {enable disable} | Enable or disable per-URL pattern web proxy forwarding and cache exemptions. | enable |
| url-pattern <pattern_str> | Enter the URL pattern. | |

wireless-controller

Use these commands to create virtual wireless access points that can be associated with multiple physical wireless access points. Clients can roam amongst the physical access points, extending the range of the wireless network.

This chapter describes the following commands:

[ap-status](#)

[global](#)

[setting](#)

[timers](#)

[vap](#)

[wids-profile](#)

[wtp](#)

[wtp-profile](#)

ap-status

Use this command to designate detected access points as accepted or rogue or to suppress a rogue AP.

To get information about detected access points, use the `get wireless-controller scan` command.

Syntax

```
config wireless-controller ap-status
  edit <ap_id>
    set bssid <bssid>
    set ssid <ssid>
    set status {accepted | rogue | suppressed}
  end
```

| Variable | Description | Default |
|--|--|-------------------|
| <ap_id> | Enter a number to identify this access point. | No default. |
| bssid <bssid> | Enter the access point's BSSID. This is the wireless AP's wireless MAC address. | 00:00:00:00:00:00 |
| ssid <ssid> | Enter the wireless service set identifier (SSID) or network name for the wireless interface. | No default. |
| status {accepted rogue suppressed} | Select the desired status for this AP: accepted or rogue. | rogue |

global

Use this command to configure global settings for physical access points, also known as WLAN Termination Points (WTPs), configured using Control And Provisioning of Wireless Access Points (CAPWAP) protocol.

Syntax

```
config wireless-controller global
  set data-ethernet-II {enable | disable}
  set dhcp-option-code <option_int>
  set discovery-mc-addr <ipv4addr>
  set local-radio-vdom <vdom_name>
  set location <string>
  set max-clients <int>
  set max-retransmit <int>
  set mesh-eth-type <id_int>
  set name <string>
  set rogue-scan-mac-adjacency <int>
end
```

| Variable | Description | Default |
|--|--|-------------|
| data-ethernet-II {enable disable} | Enable or disable use of Ethernet frame type with 802.3 data tunnel mode. | disable |
| dhcp-option-code <option_int> | Enter DHCP option code. This is available when ac-discovery-type is dhcp. | 138 |
| discovery-mc-addr <ipv4addr> | Enter the IP address for AP discovery. This is available when ac-discovery-type is multicast. | 224.0.1.140 |
| local-radio-vdom <vdom_name> | Select the VDOM to which the FortiWiFi unit's built-in access point belongs. | root |
| location <string> | Enter the location of your wireless network. | No default. |
| max-clients <int> | Enter the maximum number of clients permitted to connect simultaneously. Enter 0 for no limit. | 0 |
| max-retransmit <int> | Enter the maximum number of retransmissions for tunnel packet. Range 0 to 64. | 3 |
| mesh-eth-type <id_int> | Identifier included in packets. Useful for debugging. | 8755 |
| name <string> | Enter a name for your wireless network. | No default. |
| rogue-scan-mac-adjacency <int> | Enter the maximum numeric difference between an AP's Ethernet and wireless MAC values to match for rogue detection. Range: 0-7. | 7 |

setting

Use this command to configure VDOM-specific options for the wireless controller.

Syntax

```
config wireless-controller setting
    set ap-auto-suppress {enable | disable}
    set ap-bgscan-disable-day <day_list_str>
    set ap-bgscan-disable-end <time_str>
    set ap-bgscan-disable-start <time_str>
    set ap-bgscan-period <secs_int>
    set ap-scan {enable | disable}
    set country <country-code>
    set on-wire-scan {enable | disable}
end
```

| Variable | Description | Default |
|---|--|---------|
| ap-auto-suppress {enable disable} | Enable or disable automatic suppression of detected rogue APs. To enable ap-auto-suppress, first ap-scan and on-wire-scan must be enabled. | disable |
| ap-bgscan-disable-day <day_list_str> | Enter the days of the week when background scanning is disabled. | null |
| ap-bgscan-disable-end <time_str> | Enter the end time (format hh:mm) for disabled background scanning. ap-bgscan-disable-day must be set. | 00:00 |
| ap-bgscan-disable-start <time_str> | Enter the start time (format hh:mm) for disabled background scanning. ap-bgscan-disable-day must be set. | 00:00 |
| ap-bgscan-period <secs_int> | Enter the period in seconds between background scans. | 600 |
| ap-scan {enable disable} | Enable or disable scanning for other APs available at your location. | disable |
| country <country-code> | Select the country of operation for your wireless network. This affects the radio channels that are available. To view the available country codes, enter <code>set country ?</code> You must set the country before you configure access point (WTP) profiles. | US |
| on-wire-scan {enable disable} | Enable or disable looking for MAC addresses of unknown APs on the wired network to distinguish rogues from neighbors. Use this in conjunction with ap-scan. | disable |

timers

Use this command to alter global timers for physical access points, also known as WLAN Termination Points (WTPs) configured using Control And Provisioning of Wireless Access Points (CAPWAP) protocol.

Syntax

```
config wireless-controller timers
  set client-idle-timeout <seconds>
  set darrp-optimize <seconds_int>
  set darrp-wtp-tune <seconds_int>
  set discovery-interval <seconds>
  set echo-interval <seconds>
  set fake-ap-log <int>
  set rogue-ap-log <int>
end
```

| Variable | Description | Default |
|----------------------------------|--|---------|
| client-idle-timeout <seconds> | Set the timeout period in seconds for inactive clients. Range: 20 to 3600, 0 for no timeout. | 300 |
| darrp-optimize <seconds_int> | Set the DARRP (Dynamic Automatic Radio Resource Provisioning) optimization interval. Range: 0 to 86 400 seconds. | 1800 |
| darrp-wtp-tune <seconds_int> | Set the automatic channel selection interval. Range: 1 to 30 seconds. | 3 |
| discovery-interval <seconds> | Set the period between discovery requests. Range 2 to 180 seconds. | 5 |
| echo-interval <seconds> | Set the interval before WTP sends Echo Request after joining AC. Range 1 to 600 seconds. | 30 |
| fake-ap-log <int> | Set a period, in minutes, for periodic logging of fake APs. | 1 |
| rogue-ap-log <int> | Set a period, in minutes, for periodic logging of rogue APs. | 0 |

vap

Use this command to configure Virtual Access Points.

Syntax

```
config wireless-controller vap
edit <vap_name>
    set auth {usergroup | radius}
    set broadcast-suppression {arp | dhcp}
    set broadcast-ssid {enable | disable}
    set dynamic-vlan {enable | disable}
    set encrypt {AES | TKIP | TKIP-AES}
    set external-fast-roaming {enable | disable}
    set fast-roaming {enable | disable}
    set gtk-rekey-intv <secs>
    set intra-vap-privacy {enable | disable}
    set key <key_str>
    set keyindex {1 | 2 | 3 | 4}
    set local-authentication {enable | disable}
    set local-bridging {enable | disable}
    set local-switching {enable | disable}
    set max-clients <int>
    set mesh-backhaul {enable | disable}
    set me-disable-thresh <limit_int>
    set multicast-enhance {enable | disable}
    set passphrase <hex_str>
    set portal-message-override-group <repl-msg-group_name>
    set ptk-rekey-intv <secs>
    set radius-server <server_name>
    set radius-mac-auth {enable | disable}
    set radius-mac-auth-server <srv_str>
    set security {captive-portal | open | wep128 | wep64
        | wpa-enterprise | wpa-only-enterprise | wpa-only-personal
        | wpa-personal | wpa2-only-enterprise | wpa2-only-personal}
    set selected-usergroups <groups_str>
    set ssid <string>
    set usergroup <group_name>
    set vdom <vdom_name>
    set vlanid <vlan_int>
    set vlan-auto {enable | disable}
```

| Variable | Description | Default |
|------------------------------------|---|-----------|
| auth {usergroup radius} | Select whether WPA-Enterprise authentication uses FortiGate user groups or a RADIUS server. | usergroup |
| broadcast-suppression {arp dhcp} | Prevent ARP or DHCP messages being carried to other access points carrying the same SSID. | dhcp arp |

| Variable | Description | Default |
|---|---|-------------|
| broadcast-ssid {enable disable} | Enable broadcast of the SSID. Broadcasting the SSID enables clients to connect to your wireless network without first knowing the SSID. For better security, do not broadcast the SSID. | enable |
| dynamic-vlan {enable disable} | Enable dynamic VLAN assignment for users based RADIUS attribute. | disable |
| encrypt {AES TKIP TKIP-AES} | Select whether VAP uses AES or TKIP encryption, or accepts both. This is available if <code>security</code> is a WPA type. | AES |
| external-fast-roaming {enable disable} | Enable or disable pre-authentication with external non-managed AP. | disable |
| fast-roaming {enable disable} | Enabling fast-roaming enables pre-authentication where supported by clients. | enable |
| gtk-rekey-intv <secs> | Set the WPA re-key interval. Some clients may require a longer interval. For WPA-RADIUS SSID, use <code>ptk-rekey-intv</code> . Range 60 to 864 000 seconds. | 3600 |
| intra-vap-privacy {enable disable} | Enable to block communication between clients of the same AP. | disable |
| key <key_str> | Enter the encryption key that the clients must use. For WEP64, enter 10 hexadecimal digits. For WEP128, enter 26 hexadecimal digits. This is available when <code>security</code> is a WEP type. | No default. |
| keyindex {1 2 3 4} | Many wireless clients can configure up to four WEP keys. Select which key clients must use with this access point. This is available when <code>security</code> is a WEP type. | 1 |
| local-authentication {enable disable} | Enable authentication of clients by the FortiAP unit if the wireless controller is unavailable. This applies only if <code>security</code> is a WPA-Personal mode and <code>local-bridging</code> is enabled. | disable |
| local-bridging {enable disable} | Enable or disable bridging of wireless and Ethernet interfaces on the FortiAP unit. <code>local-bridging</code> is disabled if <code>intra-vap-privacy</code> is enabled. | disable |
| local-switching {enable disable} | Enable or disable local switching of traffic on the FortiAP, not sending it to the WiFi controller. <code>local-switching</code> is disabled if <code>intra-vap-privacy</code> is enabled. | enable |
| max-clients <int> | Enter the maximum number of clients permitted to connect simultaneously. Enter 0 for no limit. | 0 |
| mesh-backhaul {enable disable} | Enable to use this Virtual Access Point as a WiFi mesh backhaul. WiFi clients cannot connect directly to this SSID. | disable |
| me-disable-thresh <limit_int> | Set the multicast enhancement threshold. Range 2 to 256 subscribers. | 32 |
| multicast-enhance {enable disable} | Enable conversion of multicast to unicast to improve performance. | disable |

| Variable | Description | Default |
|--|--|-------------|
| passphrase <hex_str> | Enter the encryption passphrase of 8 to 63 characters. This is available when <code>security</code> is a WPA type and <code>auth</code> is PSK. | No default. |
| portal-message-override-group <repl-msg-group_name> | Enter the replacement message group for this virtual access point. The replacement message group must already exist in <code>system replacemsg-group</code> and its <code>group-type</code> must be <code>captive-portal</code> . This field is available when <code>security</code> is <code>captive-portal</code> . | Null. |
| ptk-rekey-intv <secs> | Set the WPA-RADIUS re-key interval. Some clients may require a longer interval. Range 60 to 864 000 seconds. | 3600 |
| radius-server <server_name> | Enter the RADIUS server used to authenticate users. This is available when <code>auth</code> is <code>radius</code> . | No default. |
| radius-mac-auth {enable disable} | Enable if you want MAC address authentication of clients. This is independent of other authentication protocols. You will also have to specify <code>radius-mac-auth-server</code> . | disable |
| radius-mac-auth-server <srv_str> | Specify the RADIUS server to use for MAC address authentication. This is available if <code>radius-mac-auth</code> is enabled. | null |

| Variable | Description | Default |
|--|--|--------------|
| security { captive-portal open wep128 wep64 wpa-enterprise wpa-only-enterprise wpa-only-personal wpa-personal wpa2-only-enterprise wpa2_only-personal } | <p>Select the security mode for the wireless interface. Wireless users must use the same security mode to be able to connect to this wireless interface.</p> <p><code>captive-portal</code> — users are authenticated through a captive web portal.</p> <p><code>open</code> — has no security. Any wireless user can connect to the wireless network.</p> <p><code>wep128</code> — 128-bit WEP. To use WEP128 you must enter a Key containing 26 hexadecimal digits (0-9 a-f) and inform wireless users of the key.</p> <p><code>wep64</code> — 64-bit web equivalent privacy (WEP). To use WEP64 you must enter a Key containing 10 hexadecimal digits (0-9 a-f) and inform wireless users of the key.</p> <p><code>wpa-enterprise</code> — WPA-Enterprise security, WPA or WPA2.</p> <p><code>wpa-only-enterprise</code> — WPA-Enterprise security, WPA only.</p> <p><code>wpa-only-personal</code> — WPA-Personal security, WPA only.</p> <p><code>wpa-personal</code> — WPA-Personal security, WPA or WPA2.</p> <p><code>wpa2-only-enterprise</code> — WPA-Enterprise security, WPA2 only.</p> <p><code>wpa2-only-personal</code> — WPA-Personal security, WPA2 only.</p> | wpa-personal |
| selected-usergroups <groups_str> | Select the user groups that can authenticate. This is available when <code>security</code> is <code>captive-portal</code> . | No default. |
| ssid <string> | Enter the wireless service set identifier (SSID) or network name for this wireless interface. Users who want to use the wireless network must configure their computers with this network name. | fortinet |
| usergroup <group_name> | Enter the usergroup for WPA-Enterprise authentication when <code>auth</code> is <code>usergroup</code> . | No default. |
| <vap_name> | Enter a name for this Virtual Access Point. | No default. |
| vdom <vdom_name> | Enter the name of the VDOM to which this VAP belongs. | No default. |
| vlanid <vlan_int> | Enter the VLAN ID, if a VLAN will be used. 0 means no VLAN. | 0 |
| vlan-auto { enable disable } | Enable or disable automatic VLAN assignment for authenticated users of this SSID. This is available if <code>security</code> is WPA Enterprise or captive portal and <code>vlanid</code> is not 0. | disable |

wids-profile

Use this command to configure Wireless Intrusion Detection (WIDS) profiles.

Syntax

```
config wireless-controller wids-profile
edit <wids-profile_name>
    set comment <comment_str>
    set asleap-attack {enable | disable}
    set assoc-frame-flood {enable | disable}
    set auth-frame-flood {enable | disable}
    set deauth-broadcast {enable | disable}
    set eapol-fail-flood {enable | disable}
    set eapol-fail-intv <int>
    set eapol-fail-thres <int>
    set eapol-logoff-flood {enable | disable}
    set eapol-logoff-intv <int>
    set eapol-logoff-thres <int>
    set eapol-pre-fail-flood {enable | disable}
    set eapol-pre-fail-intv <int>
    set eapol-pre-fail-thres <int>
    set eapol-pre-succ-flood {enable | disable}
    set eapol-pre-succ-intv <int>
    set eapol-pre-succ-thres <int>
    set eapol-start-flood {enable | disable}
    set eapol-start-intv <int>
    set eapol-start-thres <int>
    set eapol-succ-flood {enable | disable}
    set eapol-succ-intv <int>
    set eapol-succ-thres <int>
    set invalid-mac-oui {enable | disable}
    set long-duration-attack {enable | disable}
    set long-duration-thresh <int>
    set null-ssid-probe-resp {enable | disable}
    set spoofed-deauth {enable | disable}
    set weak-wep-iv {enable | disable}
    set wireless-bridge {enable | disable}
end
```

| Variable | Description | Default |
|---|--|-------------|
| <wids-profile_name> | Enter a name for this WIDS profile. | No default. |
| comment <comment_str> | Optionally, enter a descriptive comment. | No default. |
| asleap-attack {enable disable} | Enable to detect asleap attack (attempt to crack LEAP security). | disable |
| assoc-frame-flood {enable disable} | Enable to detect association frame flood attack. | disable |
| auth-frame-flood {enable disable} | Enable to detect authentication frame flood attack. | disable |

| Variable | Description | Default |
|---|---|---------|
| deauth-broadcast { enable disable } | | disable |
| eapol-fail-flood { enable disable } | Enable to detect EAP FAIL flood attack. | disable |
| eapol-fail-intv <int> | Set EAP FAIL detection interval. | 1 |
| eapol-fail-thres <int> | Set EAP FAIL detection threshold. | 10 |
| eapol-logoff-flood { enable disable } | Enable to detect EAP LOGOFF flood attack. | disable |
| eapol-logoff-intv <int> | Set EAP LOGOFF detection interval. | 1 |
| eapol-logoff-thres <int> | Set EAP LOGOFF detection threshold. | 10 |
| eapol-pre-fail-flood { enable disable } | Enable to detect EAP premature FAIL flood attack. | disable |
| eapol-pre-fail-intv <int> | Set EAP premature FAIL detection interval. | 1 |
| eapol-pre-fail-thres <int> | Set EAP premature FAIL detection threshold. | 10 |
| eapol-pre-succ-flood { enable disable } | Enable to detect EAP premature SUCC flood attack. | disable |
| eapol-pre-succ-intv <int> | Set EAP premature SUCC detection interval. | 1 |
| eapol-pre-succ-thres <int> | Set EAP premature SUCC detection threshold. | 10 |
| eapol-start-flood { enable disable } | Enable to detect EAP START flood attack. | disable |
| eapol-start-intv <int> | Set EAP START detection interval. | 1 |
| eapol-start-thres <int> | Set EAP START detection threshold. | 10 |
| eapol-succ-flood { enable disable } | Enable to detect EAP SUCC flood attack. | disable |
| eapol-succ-intv <int> | Set EAP SUCC detection interval. | 1 |
| eapol-succ-thres <int> | Set EAP SUCC detection threshold. | 10 |
| invalid-mac-oui { enable disable } | Enable to detect use of spoofed MAC addresses. (The first three bytes should indicate a known manufacturer.) | disable |
| long-duration-attack { enable disable } | Enable for long duration attack detection based on long-duration-thresh. | disable |
| long-duration-thresh <int> | Enter the duration in usec for long-duration attack detection. This is available when long-duration-attack is enable. | 8200 |
| null-ssid-probe-resp { enable disable } | | disable |
| spoofed-deauth { enable disable } | Enable to detect spoofed deauthentication packets. | disable |
| weak-wep-iv { enable disable } | Enable to detect APs using weak WEP encryption. | disable |
| wireless-bridge { enable disable } | Enable to detect wireless bridge operation, which is suspicious if your network doesn't use a wireless bridge. | disable |
| Read-only variables (view using get command) | | |
| used-by | | |

wtp

Use this command to configure physical access points (APs) for management by the wireless controller, also known as an access controller (AC).

Syntax

```
config wireless-controller wtp
  edit <wtp-id>
    set admin <admin_status>
    set ap-scan {enable | disable}
    set auto-power-level {enable | disable}
    set auto-power-low <dBm_int>
    set auto-power-high <dBm_int>
    set band {2.4GHz | 5GHz}
    set coordinate-enable {enable | disable}
    set coordinate-x <int>
    set coordinate-y <int>
    set image-download {enable | disable}
    set ip-fragment-preventing [icmp-unreachable tcp-mss-adjust]
    set location <string>
    set login-enable {default | enable | disable}
    set login-passwd <pwd_string>
    set login-passwd-change {default | yes | no}
    set mesh-bridge-enable {default | enable | disable}
    set name <string>
    set power-level <int>
    set radio-enable {enable | disable}
    set tun-mtu-downlink {0 | 576 | 1500}
    set tun-mtu-uplink {0 | 576 | 1500}
    set vap-all {enable | disable}
    set vaps {vap1 ... vapn}
    set vlanid <vlanid_int>
    set wtp-id <id_string>
    set wtp-profile <name_string>
  config lan
    set port1-mode {offline | bridge-to-ssid | bridge-to-wan}
    set port1-ssid <ssid_name>
  end
end
```

To retrieve information about a physical access point:

```
config wireless-controller wtp
  edit <wtp-id>
    get
  end
```

Along with the current configuration settings, information such as the current number of clients, is returned. See the read-only variables section of the table below.

| Variable | Description | Default |
|--|--|-------------|
| edit <wtp-id> | Enter the ID for the AP unit. | No default. |
| admin <admin_status> | Set to one of the following: discovered — This is the setting for APs that have discovered this AC and registered themselves. To use such an AP, select enable. disable — Do not manage this AP. enable — Manage this AP. | enable |
| ap-scan {enable disable} | Enable or disable rogue AP scanning. | enable |
| auto-power-level {enable disable} | Enable or disable automatic power-level adjustment to prevent co-channel interference. | disable |
| auto-power-low <dBm_int> | Set automatic power level low limit, in dBm. Range 0 to 17dBm. | 10 |
| auto-power-high <dBm_int> | Set automatic power level high limit, in dBm. Range 0 to 17dBm. | 17 |
| band {2.4GHz 5GHz} | Select 2.4GHz or 5GHz band. Applies when automatic profile is used. | 2.4GHz |
| coordinate-enable {enable disable} | Enable AP unit coordinates. | disable |
| coordinate-x <int> coordinate-y <int> | Enter x and y coordinates for AP. This is available if coordinate-enable is enabled. | 0,0 |
| image-download {enable disable} | Enable or disable downloading of firmware to the AP unit. | enable |
| ip-fragment-preventing [icmp-unreachable tcp-mss-adjust] | Enable options to deal with CAPWAP packet fragmentation: icmp-unreachable — drop packet, send ICMP Destination unreachable tcp-mss-adjust — adjust MTU using tun-mtu-uplink and tun-mtu-downlink | null |
| location <string> | Optionally, enter the location of this AP. | No default. |
| login-enable {default enable disable} | Enable or disable AP telnet login. Set to default to control the AP telnet login capability with the TELNET_ALLOW setting on the AP unit. | default |
| login-passwd <pwd_string> | Set the AP unit login password. This is available if login-passwd-change is yes. | No default. |
| login-passwd-change {default yes no} | Select whether to change AP unit login password. Select default to change the AP unit password back to its default. | no |
| mesh-bridge-enable {default enable disable} | Enable to create a bridge between the AP unit's WiFi interface and its Ethernet interface. Set to default to use the setting configured on the FortiAP unit. | disable |
| name <string> | Enter a name to identify this access point. | No default. |

| Variable | Description | Default |
|---|--|-------------|
| power-level <int> | Set radio power level. Range is 0 (minimum) to 100 (maximum). The maximum power level is set to the regulatory maximum for your region, as determined by your selection in the <code>country</code> field of wireless-controller setting . | 100 |
| radio-enable { enable disable } | Enable or disable radio operation. | enable |
| tun-mtu-downlink { 0 576 1500 } | Set CAPWAP uplink MTU to 576 or 1500, or leave alone (0). | 0 |
| tun-mtu-uplink { 0 576 1500 } | Set CAPWAP downlink MTU to 576 or 1500, or leave alone (0). | 0 |
| vap-all { enable disable } | Enable to inherit all VAPs. Disable to select VAPs. | enable |
| vaps { vap1 ... vapn } | Set the virtual access points carried on this physical access point. This is used only when <code>wtp-profile</code> is not set. | No default. |
| vlanid <vlanid_int> | Optionally assign a VLAN ID for local bridge VAP traffic. | 0 |
| wtp-id <id_string> | Enter the ID of the AP unit. | No default. |
| wtp-profile <name_string> | Enter the name of the wtp profile to apply to this access point. | No default. |
| config lan variables | | |
| port1-mode { offline bridge-to-ssid bridge-to-wan } | Set FortiAP LAN port mode: <ul style="list-style-type: none"> offline — not used bridge-to-ssid — bridge with specified SSID bridge-to-wan — bridge with WAN port There is also <code>port2-mode</code> , <code>port3-mode</code> , etc., depending on the number of independent LAN interfaces on the FortiAP unit. | offline |
| port1-ssid <ssid_name> | Enter the SSID to bridge with LAN port 1. This is available when <code>port1-mode</code> is <code>bridge-to-ssid</code> . There is also <code>port2-ssid</code> , <code>port3-ssid</code> , etc., depending on the number of independent LAN interfaces on the FortiAP unit. | No default. |
| Read-only variables (view using get command) | | |
| base-bssid base-bssid-2 | The wireless MAC address of each radio. | |
| client-count | The number of clients connected to this managed access point. | |
| connection-state | Shows “connected” if FortiAP is connected, otherwise “idle”. | |
| image-download-progress | Shows 0-100% progress during FortiAP image upload. | |
| join-time | Date and time that the managed AP connected to the controller. | |
| last-failure | Last error message concerning this managed AP. | |
| last-failure-param | Additional information about the last error. | |
| last-failure-time | Date and time of last error message. | |
| local-ipv4-address | The IP address assigned to the AP. | |

| Variable | Description | Default |
|--------------------------|---|---------|
| max-vaps max-vaps-2 | The maximum number of SSIDs supported on each radio. | |
| oper-chan oper-chan-2 | The current operating channel of each radio. | |
| region-code | The region-code (country) currently set on the FortiAP unit. | |
| software-version | The build number of the FortiAP firmware, e.g.:FAP22A-v4.0-build212 | |

wtp-profile

Use this command to define an access point profile (wtp profile).

Syntax

```
config wireless-controller wtp-profile
  edit <name_string>
    set ap-country <country-code>
    set comment <comment_string>
    set dtls-policy {clear-text | dtls-enabled}
    set handoff-rssi <rssi_int>
    set handof-sta-thresh <thresh_int>
    set ip-fragment-preventing [icmp-unreachable tcp-mss-adjust]
    set max-clients <int>
    set preferred-oper-mode {LE | SN}
    set tun-mtu-downlink {0 | 576 | 1500}
    set tun-mtu-uplink {0 | 576 | 1500}
  config deny-mac-list
    edit <mac_id>
      set mac <mac>
    end
  config lan
    set port1-mode {offline | bridge-to-ssid | bridge-to-wan}
    set port1-ssid <ssid_name>
  end
  config platform
    set type <type_string>
  end
  config radio-1
    set ap-auto-suppress {enable | disable}
    set ap-bgscan {enable | disable}
    set ap-bgscan-disable-day <day_list_str>
    set ap-bgscan-disable-end <time_str>
    set ap-bgscan-disable-start <time_str>
    set ap-bgscan-period <secs_int>
    set auto-power-level {enable | disable}
    set auto-power-low <dBm_int>
    set auto-power-high <dBm_int>
    set band {802.11a | 802.11b | 802.11g | 802.11n | 802.11n-5G}
    set beacon-interval <integer>
    set channel <channels_string>
    set darrp {enable | disable}
    set dtim <int>
    set frag-threshold <int>
    set max-distance <m_int>
    set max-supported-mcs <mcs_int>
    set mode <mode_string>
    set power-level <dBm>
```

```

    set protection-mode {disable | ctsonly | rtscts}
    set rts-threshold <int>
    set short-guard-interval {enable | disable}
    set station-locate {enable | disable}
    set vaps {vap1 ... vapn}
end
config radio-2
    set ap-auto-suppress {enable | disable}
    set ap-bgscan {enable | disable}
    set ap-bgscan-disable-day <day_list_str>
    set ap-bgscan-disable-end <time_str>
    set ap-bgscan-disable-start <time_str>
    set ap-bgscan-period <secs_int>
    set auto-power-level {enable | disable}
    set auto-power-low <dBm_int>
    set auto-power-high <dBm_int>
    set band {802.11a | 802.11b | 802.11g | 802.11n | 802.11n-5G}
    set beacon-interval <integer>
    set channel <channels_string>
    set channel-bonding {enable | disable}
    set darrp {enable | disable}
    set dtim <int>
    set frag-threshold <int>
    set max-distance <m_int>
    set max-supported-mcs <mcs_int>
    set mode <mode_string>
    set power-level <dBm>
    set protection-mode {disable | ctsonly | rtscts}
    set rts-threshold <int>
    set short-guard-interval {enable | disable}
    set vaps {vap1 ... vapn}
end
end

```

| Variable | Description | Default |
|--|--|-------------|
| ap-country <country-code> | Set the country in which this AP will operate. To list available country codes, enter set ap-country ? | US |
| comment <comment_string> | Optionally, enter a description. | No default. |
| dtls-policy {clear-text dtls-enabled} | Select whether CAPWAP protocol uses clear-text or DTLS encryption. | clear-text |
| handoff-rssi <rssi_int> | Enter the minimum RSSI value for handoff. | 25 |
| handof-sta-thresh <thresh_int> | Enter the threshold value for AP handoff. | 30 |

| Variable | Description | Default |
|--|---|-------------|
| ip-fragment-preventing [icmp-unreachable tcp-mss-adjust] | Enable options to deal with CAPWAP packet fragmentation: icmp-unreachable — drop packet, send ICMP Destination unreachable tcp-mss-adjust — adjust MTU using tun-mtu-uplink and tun-mtu-downlink | null |
| max-clients <int> | Enter the maximum number of clients this AP supports. Use 0 for no limit. | 0 |
| preferred-oper-mode {LE SN} | Select the preferred operating mode: <ul style="list-style-type: none">LE — local MAC and 802.3 frame tunnel modeSN — split MAC and 802.11 frame tunnel mode | LE |
| tun-mtu-downlink {0 576 1500} | Set CAPWAP uplink MTU to 576 or 1500, or leave alone (0). | 0 |
| tun-mtu-uplink {0 576 1500} | Set CAPWAP downlink MTU to 576 or 1500, or leave alone (0). | 0 |
| config deny-mac-list variables | | |
| <mac_id> | Enter a number to identify this entry. | No default. |
| mac <mac> | Enter the wireless MAC address to deny. | No default. |
| config lan variables | | |
| port1-mode {offline bridge-to-ssid bridge-to-wan} | Set FortiAP LAN port mode: <ul style="list-style-type: none">offline — not usedbridge-to-ssid — bridge with specified SSIDbridge-to-wan — bridge with WAN port There is also port2-mode, port3-mode, etc., depending on the number of independent LAN interfaces on the FortiAP unit. | offline |
| port1-ssid <ssid_name> | Enter the SSID to bridge with LAN port 1. This is available when port1-mode is bridge-to-ssid. There is also port2-ssid, port3-ssid, etc., depending on the number of independent LAN interfaces on the FortiAP unit. | No default. |
| config platform variables | | |
| type <type_string> | Enter the AP hardware type. To see a list of hardware types, enter set type ? | 220B |
| config radio-1, config radio-2 variables | | |
| ap-auto-suppress {enable disable} | Enable or disable automatic suppression of detected rogue APs. This is available only if mode is monitor. | disable |
| ap-bgscan {enable disable} | Enable or disable background scanning. Note: Scanning can reduce performance. | disable |
| ap-bgscan-disable-day <day_list_str> | Enter the days of the week when background scanning is disabled. | null |
| ap-bgscan-disable-end <time_str> | Enter the end time (format hh:mm) for disabled background scanning. ap-bgscan-disable-day must be set. | 00:00 |
| ap-bgscan-disable-start <time_str> | Enter the start time (format hh:mm) for disabled background scanning. ap-bgscan-disable-day must be set. | 00:00 |

| Variable | Description | Default |
|---|---|-------------|
| ap-bgscan-period <secs_int> | Enter the period in seconds between background scans. | 600 |
| auto-power-level { enable disable } | Enable or disable automatic power-level adjustment to prevent co-channel interference. | disable |
| auto-power-low <dBm_int> | Set automatic power level low limit, in dBm. Range 0 to 17dBm. | 10 |
| auto-power-high <dBm_int> | Set automatic power level high limit, in dBm. Range 0 to 17dBm. | 17 |
| band { 802.11a 802.11b 802.11g 802.11n 802.11n-5G } | Enter the wireless band to use. Available bands depend on the capabilities of the radio. 802.11n-5G is 802.11n on the 5GHz band. | No default. |
| beacon-interval <integer> | Set the interval between beacon packets. Access Points broadcast beacons or Traffic Indication Messages (TIM) to synchronize wireless networks. In an environment with high interference, decreasing the beacon-interval might improve network performance. In a location with few wireless nodes, you can increase this value. | 100 |
| channel <channels_string> | Enter a list of the radio channels your access point can use. Separate the channel numbers with spaces. The AP will use the least busy of the listed channels. To determine which channels are available for your selected radio band and geography, enter <code>set channel ?</code> | No default. |
| channel-bonding { enable disable } | Available for <code>config radio-2</code> only. | disable |
| darrp { enable disable } | Enable Distributed Automatic Radio Resource Provisioning. | disable |
| dtim <int> | Set the interval for Delivery Traffic Indication Message (DTIM). Range is 1 to 255. | 1 |
| frag-threshold <int> | Set the maximum packet size that can be sent without fragmentation. Range is 800 to 2346 bytes. | 2346 |
| max-distance <m_int> | Set the maximum expected distance in meters between the AP and clients. This adjusts the ACK timeout to maintain throughput at the maximum distance. Range 0 to 20 000 meters. | 0 |
| max-supported-mcs <mcs_int> | Range 0 - 31. | 15 |
| mode <mode_string> | Select one of the following modes for the access point: ap — Radio provides wireless Access Point service. monitor — Radio performs scanning only. disable — Radio is not used. | ap |
| power-level <dBm> | Set transmitter power level in dBm. Range 0 to 17. | 17 |
| protection-mode { disable ctsonly rtsets } | Select 802.11g protection mode. | disable |
| rts-threshold <int> | Set the packet size for RTS transmissions. Range 256 to 2346 bytes. | 2346 |

| Variable | Description | Default |
|--|--|-------------|
| short-guard-interval {enable disable} | Optionally, enabling this option might increase the data rate. | disable |
| station-locate {enable disable} | Enable station location for all clients, associated or not. | disable |
| vaps {vap1 ... vap <i>n</i> > | Set the virtual access points carried on this physical access point. | No default. |
| wids-profile <wids-profile_name> | Enter the WIDS profile name. | No default. |

execute

The execute commands perform immediate operations on the FortiGate unit, including:

- Maintenance operations, such as back up and restore the system configuration, reset the configuration to factory settings, update antivirus and attack definitions, set the date and time.
- Network operations, such as view and clear DHCP leases, clear arp table entries, use ping or traceroute to diagnose network problems.
- View and delete log messages. Delete old log files.
- Generate certificate requests and install certificates for VPN authentication.

This chapter contains the following sections:

| | | |
|--|---|--|
| backup | log convert-oldlogs | shutdown |
| batch | log delete-all | ssh |
| bypass-mode | log delete-oldlogs | sync-session |
| carrier-license | log display | tac report |
| central-mgmt | log filter | telnet |
| cfg reload | log fortianalyzer test-connectivity | time |
| cfg save | log list | traceroute |
| clear system arp table | log rebuild-sqldb | tracert6 |
| cli check-template-status | log recreate-sqldb | update-ase |
| cli status-msg-only | log-report reset | update-av |
| client-reputation | log roll | update-geo-ip |
| date | log upload-progress | update-ips |
| disk | modem dial | update-now |
| disk raid | modem hangup | update-src-vis |
| dhcp lease-clear | modem trigger | upd-vd-license |
| dhcp lease-list | mrrouter clear | upload |
| disconnect-admin-session | netscan | usb-device |
| enter | pbx | usb-disk |
| factoryreset | ping | vpn certificate ca |
| factoryreset2 | ping-options, ping6-options | vpn certificate cri |
| formatlogdisk | ping6 | vpn certificate local |
| forticarrier-license | policy-packet-capture delete-all | vpn certificate remote |
| forticlient | reboot | vpn ipsec tunnel down |
| fortiguard-log | report | vpn ipsec tunnel up |
| fortisandbox test-connectivity | report-config reset | vpn sslvpn del-all |
| fortitoken | restore | vpn sslvpn del-tunnel |
| fortitoken-mobile | revision | vpn sslvpn del-web |
| fsso refresh | router clear bfd session | vpn sslvpn list |
| ha disconnect | router clear bgp | webfilter quota-reset |
| ha ignore-hardware-revision | router clear ospf process | wireless-controller delete-wtp-image |
| ha manage | router restart | wireless-controller list-wtp-image |
| ha synchronize | send-fds-statistics | wireless-controller reset-wtp |
| interface dhcpclient-renew | set system session filter | wireless-controller restart-acd |
| interface pppoe-reconnect | set-next-reboot | wireless-controller restart-wtpd |
| log client-reputation-report | sfp-mode-sgmii | wireless-controller upload-wtp-image |

backup

Back up the FortiGate configuration files, logs, or IPS user-defined signatures file to a TFTP or FTP server, USB disk, or a management station. Management stations can either be a FortiManager unit, or FortiGuard Analysis and Management Service. For more information, see “[system fortiguard](#)” on page 516 or “[system central-management](#)” on page 494.

When virtual domain configuration is enabled (in `system global`, `vdom-admin` is enabled), the content of the backup file depends on the administrator account that created it.

- A backup of the system configuration from the super admin account contains the global settings and the settings for all of the VDOMs. Only the super admin can restore the configuration from this file.
- When you back up the system configuration from a regular administrator account, the backup file contains the global settings and the settings for the VDOM to which the administrator belongs. Only a regular administrator account can restore the configuration from this file.

Syntax

```
execute backup config flash <comment>
execute backup config ftp <filename_str> <server_ipv4[:port_int] |
    server_fqdn[:port_int]> [<username_str> [<password_str>]]
    [<backup_password_str>]
execute backup config management-station <comment_str>
execute backup config tftp <filename_str> <server_ipv4>
    [<backup_password_str>]
execute backup config usb <filename_str> [<backup_password_str>]
execute backup config-with-forticlient-info usb-mode
    [<backup_password_str>]
execute backup config-with-forticlient-info ftp <filename_str>
    <server_ipv4[:port_int] | server_fqdn[:port_int]>
    [<username_str> [<password_str>]] [<backup_password_str>]
execute backup config-with-forticlient-info tftp <filename_str>
    <server_ipv4> [<backup_password_str>]
execute backup config-with-forticlient-info usb
    [<backup_password_str>]
execute backup config-with-forticlient-info usb-mode
    [<backup_password_str>]
execute backup full-config ftp <filename_str> <server_ipv4[:
    port_int] | server_fqdn[:port_int]> [<username_str>
    [<password_str>]] [<backup_password_str>]
execute backup full-config tftp <filename_str> <server_ipv4>
    [<backup_password_str>]
execute backup full-config usb <filename_str>
    [<backup_password_str>]
execute backup full-config usb-mode <filename_str>
    [<backup_password_str>]
execute backup ipsuserdefsig ftp <filename_str> <server_ipv4[:
    port_int] | server_fqdn[:port_int]> [<username_str>
    [<password_str>]]
execute backup ipsuserdefsig tftp tftp <filename_str> <server_ipv4>
execute backup {disk | memory} alllogs ftp <server_ipv4[:port_int] |
    server_fqdn[:port_int]> [<username_str> <password_str>]
```

```

execute backup {disk | memory} alllogs tftp <server_ipv4>
execute backup {disk | memory} log ftp <server_ipv4[:port_int] |
server_fqdn[:port_int]> <username_str> <password_str> {traffic
| event | ids | virus | webfilter | spam | dlp | voip | app-ctrl
| netscan}
execute backup {disk | memory} log {ftp | tftp} <server_ipv4> netscan

```

| Variable | Description |
|---|---|
| config flash <comment> | Back up the system configuration to the flash disk. Optionally, include a comment. |
| config ftp <filename_str> <server_ipv4[:port_int] server_fqdn[:port_int]> [<username_str> [<password_str>]] [<backup_password_str>] | Back up the system configuration to an FTP server. Optionally, you can specify a password to protect the saved data. |
| config management-station <comment_str> | Back up the system configuration to a configured management station. If you are adding a comment, do not add spaces, underscore characters (_), or quotation marks (" ") or any other punctuation marks. For example, uploadedthetransparentmodeconfigfortheaccountingdepartmentwilluploadonadailybasis. The comment you enter displays in both the portal website and FortiGate web-based manager (System > Maintenance > Revision). |
| config tftp <filename_str> <server_ipv4> [<backup_password_str>] | Back up the system configuration to a file on a TFTP server. Optionally, you can specify a password to protect the saved data. |
| config usb <filename_str> [<backup_password_str>] | Back up the system configuration to a file on a USB disk. Optionally, you can specify a password to protect the saved data. |
| config usb-mode [<backup_password_str>] | Back up the system configuration to a USB disk (Global admin only). Optionally, you can specify a password to protect the saved data. |
| config-with-forticlient-info ftp <filename_str> <server_ipv4[:port_int] server_fqdn[:port_int]> [<username_str> [<password_str>]] [<backup_password_str>] | Back up the system configuration to a file on an FTP server. Optionally, you can specify a password to protect the saved data. |
| config-with-forticlient-info tftp <filename_str> <server_ipv4> [<backup_password_str>] | Back up the system configuration to a file on a TFTP server. Optionally, you can specify a password to protect the saved data. |
| config-with-forticlient-info usb [<backup_password_str>] | Back up the system configuration to a file on a USB disk. Optionally, you can specify a password to protect the saved data. |
| config-with-forticlient-info usb-mode [<backup_password_str>] | Back up the system configuration to a USB disk (Global admin only). Optionally, you can specify a password to protect the saved data. |
| full-config ftp <filename_str> <server_ipv4[:port_int] server_fqdn[:port_int]> [<username_str> [<password_str>]] [<backup_password_str>] | Back up the full system configuration to a file on an FTP server. You can optionally specify a password to protect the saved data. |

| Variable | Description |
|--|---|
| full-config tftp <filename_str> <server_ipv4> [<backup_password_str>] | Back up the full system configuration to a file on a TFTP server. You can optionally specify a password to protect the saved data. |
| full-config usb <filename_str> [<backup_password_str>] | Back up the full system configuration to a file on a USB disk. You can optionally specify a password to protect the saved data. |
| full-config usb-mode <filename_str> [<backup_password_str>] | Back up the full system configuration to a file on a USB disk (Global admin only). You can optionally specify a password to protect the saved data. |
| ipsuserdefsig ftp <filename_str> <server_ipv4[:port_int] server_fqdn[:port_int]> [<username_str> [<password_str>]] | Backup IPS user-defined signatures to a file on an FTP server. |
| ipsuserdefsig tftp tftp <filename_str> <server_ipv4> | Back up IPS user-defined signatures to a file on a TFTP server. |
| {disk memory} alllogs ftp <server_ipv4[:port_int] server_fqdn[:port_int]> [<username_str> <password_str>] | Back up either all memory or all hard disk log files for this VDOM to an FTP server. The disk option is available on FortiGate models that log to a hard disk. The file name has the form: <log_file_name>_<VDOM>_<date>_<time> |
| {disk memory} alllogs tftp <server_ipv4> | Back up either all memory or all hard disk log files for this VDOM to a TFTP server. The disk option is available on FortiGate models that log to a hard disk. The file name has the form: <log_file_name>_<VDOM>_<date>_<time> |
| {disk memory} log ftp <server_ipv4[:port_int] server_fqdn[:port_int]> <username_str> <password_str> {traffic event ids virus webfilter spam dlp voip app-ctrl netscan} | Back up the specified type of log file from either hard disk or memory to an FTP server. The disk option is available on FortiGate models that log to a hard disk. |
| {disk memory} log tftp <server_ipv4> {traffic event ids virus webfilter spam dlp voip app-ctrl netscan} | Back up the specified type of log file from either hard disk or memory to an FTP server. The disk option is available on FortiGate models that log to a hard disk. |
| {disk memory} log {ftp tftp} <server_ipv4> netscan | Back up the specified type of log file from either hard disk or memory to FTP or TFTP server. The disk option is available on FortiGate models that log to a hard disk. |

Example

This example shows how to backup the FortiGate unit system configuration to a file named `fgt.cfg` on a TFTP server at IP address 192.168.1.23.

```
execute backup config tftp fgt.cfg 192.168.1.23
```

batch

Execute a series of CLI commands.



`execute batch` commands are controlled by the Maintenance (`mntgrp`) access control group.

Syntax

```
execute batch [<cmd_cue>]
```

where `<cmd_cue>` is one of:

- `end` — exit session and run the batch commands
- `lastlog` — read the result of the last batch commands
- `start` — start batch mode
- `status` — batch mode status reporting if batch mode is running or stopped

Example

To start batch mode:

```
execute batch start
Enter batch mode...
```

To enter commands to run in batch mode:

```
config system global
    set refresh 5
end
```

To execute the batch commands:

```
execute batch end
Exit and run batch commands...
```

bypass-mode

Use this command to manually switch a FortiGate-600C or FortiGate-1000C into bypass mode. This is available in transparent mode only. If manually switched to bypass mode, the unit remains in bypass-mode until bypass mode is disabled.

Syntax

```
execute bypass-mode {enable | disable}
```

carrier-license

Use this command to enter a FortiOS Carrier license key if you have installed a FortiOS Carrier build on a FortiGate unit and need to enter a license key to enable FortiOS Carrier functionality.

Contact Fortinet Support for more information about this command.

Syntax

```
execute carrier-license <license_key>
```

| Variable | Description |
|---------------|---|
| <license_key> | Enter the FortiOS Carrier license key supplied by Fortinet. |

central-mgmt

Update Central Management Service account information. Also used receive configuration file updates from an attached FortiManager unit.

Syntax

```
execute central-mgmt set-mgmt-id <management_id>
execute central-mgmt register-device <fmg-serial-number>
    <fmg-register-password> <fgt-user-name> <fgt-password>
execute central-mgmt unregister-device <fmg-serial-number>
```

`set-mgmt-id` is used to change or initially set the management ID, or your account number for Central Management Services. This account ID must be set for the service to be enabled.

`register-device` registers the FortiGate unit with a specific FortiManager unit specified by serial number. You must also specify the administrator name and password that the FortiManager unit uses to log on to the FortiGate unit.

`unregister-device` removes the FortiGate unit from the specified FortiManager unit's device list.

`update` is used to update your Central Management Service contract with your new management account ID. This command is to be used if there are any changes to your management service account.

Example

If you are registering with the Central Management Service for the first time, and your account number is 123456, you would enter the following:

```
execute central-mgmt set-mgmt-id 123456
```

cfg reload

Use this command to restore the saved configuration when the configuration change mode is `manual` or `revert`. This command has no effect if the mode is `automatic`, the default. The `set cfg-save` command in `system global` sets the configuration change mode.

When you reload the saved system configuration, the your session ends and the FortiGate unit restarts.

In the default configuration change mode, `automatic`, CLI commands become part of the saved unit configuration when you execute them by entering either `next` or `end`.

In `manual` mode, commands take effect but do not become part of the saved configuration unless you execute the `execute cfg save` command. When the FortiGate unit restarts, the saved configuration is loaded. Configuration changes that were not saved are lost.

The `revert` mode is similar to `manual` mode, except that configuration changes are saved automatically if the administrative session is idle for more than a specified timeout period. This provides a way to recover from an erroneous configuration change, such as changing the IP address of the interface you are using for administration. You set the timeout in `system global` using the `set cfg-revert-timeout` command.

Syntax

```
execute cfg reload
```

Example

This is sample output from the command when successful:

```
# execute cfg reload
configs reloaded. system will reboot.This is sample output from the
    command when not in runtime-only configuration mode:
# execute cfg reload
no config to be reloaded.
```

cfg save

Use this command to save configuration changes when the configuration change mode is `manual` or `revert`. If the mode is `automatic`, the default, all changes are added to the saved configuration as you make them and this command has no effect. The `set cfg-save` command in `system global` sets the configuration change mode.

In `manual` mode, commands take effect but do not become part of the saved configuration unless you execute the `execute cfg save` command. When the FortiGate unit restarts, the saved configuration is loaded. Configuration changes that were not saved are lost.

The `revert` mode is similar to `manual` mode, except that configuration changes are reverted automatically if the administrative session is idle for more than a specified timeout period. This provides a way to recover from an erroneous configuration change, such as changing the IP address of the interface you are using for administration. To change the timeout from the default of 600 seconds, go to `system global` and use the `set cfg-revert-timeout` command.

Syntax

```
execute cfg save
```

Example

This is sample output from the command:

```
# execute cfg save
config saved.
```

This is sample output when not in runtime-only configuration mode. It also occurs when in runtime-only configuration mode and no changes have been made:

```
# execute cfg save
no config to be saved.
```

clear system arp table

Clear all the entries in the arp table.

Syntax

```
execute clear system arp table
```

cli check-template-status

Reports the status of the secure copy protocol (SCP) script template.

Syntax

```
execute cli check-template-status
```

cli status-msg-only

Enable or disable displaying standardized CLI error output messages. If executed, this command stops other debug messages from displaying in the current CLI session. This command is used for compatibility with FortiManager.

Syntax

```
execute cli status-msg-only [enable | disable]
```

| Variable | Description | Default |
|---------------------------------------|---|---------|
| status-msg-only [enable disable] | Enable or disable standardized CLI error output messages. Entering the command without enable or disable disables displaying standardized output. | enable |

client-reputation

Use these commands to retrieve or remove client reputation information.

Syntax

To erase all client reputation data

```
execute client-reputation erase
```

To retrieve client reputation host count

```
execute client-reputation host-count <rows>
```

To retrieve client reputation host details

```
execute client-reputation host detail <host>
```

To retrieve client reputation host summary

```
execute client-reputation host summary <host>
```

To purge old data

```
execute client-reputation purge
```

To view the top *n* records

```
execute client-reputation <n | all>
```

date

Get or set the system date.

Syntax

```
execute date [<date_str>]
```

`date_str` has the form `yyyy-mm-dd`, where

- `yyyy` is the year and can be 2001 to 2037
- `mm` is the month and can be 01 to 12
- `dd` is the day of the month and can be 01 to 31

If you do not specify a date, the command returns the current system date. Shortened values, such as '06' instead of '2006' for the year or '1' instead of '01' for month or day, are not valid.

Example

This example sets the date to 17 September 2004:

```
execute date 2004-09-17
```


disk

Use this command to list and format hard disks installed in FortiGate units or individual partitions on these hard disks.

Syntax

```
execute disk format <partition1_ref_int> [...<partitionn_ref_int>]  
execute disk list
```

| Variable | Description |
|-----------|---|
| format | Format the referenced disk partitions or disks. Separate reference numbers with spaces. If you enter a partition reference number the disk partition is formatted. If you enter a disk reference number the entire disk and all of its partitions are formatted. |
| list | List the disks and partitions and the reference number for each one. |
| <ref_int> | Disk (device) or partition reference number. |

The `execute disk format` command formats the specified partitions or disks and then reboots the system if a reboot is required.

In most cases you need to format the entire disk only if there is a problem with the partition. Formatting the partition removes all data from the partition. Formatting the disk removes all data from the entire disk and creates a single partition on the disk.

Examples

Use the following command to list the disks and partitions.

```
execute disk list
```

```
Device I1          29.9 GB      ref: 256      SUPER TALENT (IDE)  
  partition 1      29.9 GB      ref: 257      label: 224E6EE7177E1652
```

In this example (for a FortiGate-51B), the disk (device) reference number is 256 and the reference number for the single partition is 257.

Enter the following command to format the partition.

```
execute disk format 257
```

After a confirmation message the FortiGate unit formats the partition and restarts. This can take a few minutes.

Enter the following command to format the entire disk.

```
execute disk format 256
```

After a confirmation message the FortiGate unit formats the disk, restores the original partition, and restarts. This can take a few minutes.

disk raid

Use this command to view information about and change the raid settings on FortiGate units that support RAID.

Syntax

```
execute disk raid disable
execute disk raid enable {Raid-0 | Raid-1 | Raid-5}
execute disk raid rebuild
execute disk raid status
```

| Variable | Description |
|--------------------------------------|---|
| disable | Disable raid for the FortiGate unit. |
| enable {Raid-0 Raid-1 Raid-5} | Change the RAID level on the FortiGate unit. |
| rebuild | Rebuild RAID on the FortiGate unit at the same RAID level. You can only execute this command if a RAID error has been detected. Changing the RAID level takes a while and deletes all data on the disk array. |
| status | Display information about the RAID disk array in the FortiGate unit. |

Examples

Use the following command to display information about the RAID disk array in a FortiGate-82C.

```
execute disk raid status
RAID Level: Raid-1
RAID Status: OK
RAID Size: 1000GB

Disk 1:          OK          Used          1000GB
Disk 2:          OK          Used          1000GB
Disk 3:          OK          Used          1000GB
Disk 4:  Unavailable  Not-Used          0GB
```

dhcp lease-clear

Clear all DHCP address leases.

Syntax

For IPv4:

```
execute dhcp lease-clear
```

For IPv6

```
execute dhcp6 lease-clear
```

dhcp lease-list

Display DHCP leases on a given interface

Syntax

For IPv4:

```
execute dhcp lease-list [interface_name]
```

For IPv6:

```
execute dhcp6 lease-list [interface_name]
```

If you specify an interface, the command lists only the leases issued on that interface. Otherwise, the list includes all leases issued by DHCP servers on the FortiGate unit.

If there are no DHCP leases in use on the FortiGate unit, an error will be returned.

disconnect-admin-session

Disconnect an administrator who is logged in.

Syntax

```
execute disconnect-admin-session <index_number>
```

To determine the index of the administrator that you want to disconnect, view the list of logged-in administrators by using the following command:

```
execute disconnect-admin-session ?
```

The list of logged-in administrators looks like this:

Connected:

| INDEX | USERNAME | TYPE | FROM | TIME |
|-------|----------|------|--------------------|---------------------|
| 0 | admin | WEB | 172.20.120.51 | Mon Aug 14 12:57:23 |
| | 2006 | | | |
| 1 | admin2 | CLI | ssh(172.20.120.54) | Mon Aug 14 12:57:23 |
| | 2006 | | | |

Example

This example shows how to disconnect the logged administrator `admin2` from the above list.

```
execute disconnect-admin-session 1
```

enter

Use this command to go from global commands to a specific virtual domain (VDOM).

Only available when virtual domains are enabled and you are in config global.

After you enter the VDOM, the prompt will not change from “(global)”. However you will be in the VDOM with all the commands that are normally available in VDOMs.

Syntax

```
execute enter <vdom>
```

Use “?” to see a list of available VDOMs.

erase-disk

Use this command to reformat the boot device or an attached hard disk. Optionally, this command can restore the image from a TFTP server after erasing.

Syntax

```
execute erase-disk <disk_name>
```

The <disk_name> for the boot device is boot.

factoryreset

Reset the FortiGate configuration to factory default settings.

Syntax

```
execute factoryreset [keepvmlicense]
```

If `keepvmlicense` is specified (VM models only), the VM license is retained after reset.

Apart from the `keepvmlicense` option, this procedure deletes all changes that you have made to the FortiGate configuration and reverts the system to its original configuration, including resetting interface addresses.

factoryreset2

Reset the FortiGate configuration to factory default settings except VDOM and interface settings.

Syntax

```
execute factoryreset2 [keepvmlicense]
```

If `keepvmlicense` is specified (VM models only), the VM license is retained after reset.

formatlogdisk

Format the FortiGate hard disk to enhance performance for logging.

Syntax

```
execute formatlogdisk
```



In addition to deleting logs, this operation will erase all other data on the disk, including system configuration, quarantine files, and databases for antivirus and IPS.

forticarrier-license

Use this command to perform a FortiCarrier license upgrade.

Syntax

```
execute forticarrier-license <activation-code>
```

forticlient

Use these commands to manage FortiClient licensing.

Syntax

To view FortiClient license information

```
execute forticlient info
```

To show current FortiClient count

```
execute forticlient list <connection_type>
```

where <connection_type> is one of:

- 0 - IPsec
- 1 - SSLVPN
- 2 - NAC (Endpoint Security)
- 3 - WAN optimization
- 4 - Test

fortiguard-log

Use this to manage FortiGuard Analysis and Management Service (FortiCloud) operation.

Syntax

To create a FortiCloud account

```
execute fortiguard-log create-account
```

To activate FortiCloud certification

```
execute fortiguard-log certification
```

To retrieve the FortiCloud agreement

```
execute fortiguard-log agreement
```

To log in to a FortiCloud account

```
execute fortiguard-log login <account-id> <password>
```

To update the FortiGuard Analysis and Management Service contract

```
execute fortiguard-log update
```

fortisandbox test-connectivity

Use this command to query FortiSandbox connection status.

Syntax

```
execute fortisandbox test-connectivity
```

fortitoken

Use these commands to activate and synchronize a FortiToken device. FortiToken devices are used in two-factor authentication of administrator and user account logons. The device generates a random six-digit code that you enter during the logon process along with user name and password.

Before they can be used to authenticate account logins, FortiToken devices must be activated with the FortiGuard service. When successfully activated, the status of the FortiToken device will change from New to Active.

Synchronization is sometimes needed due to the internal clock drift of the FortiToken device. It is not unusual for new FortiToken units to require synchronization before being put into service. Synchronization is accomplished by entering two sequential codes provided by the FortiToken.

Syntax

To activate one or more FortiToken devices

```
execute fortitoken activate <serial_number> [serial_number2 ...  
serial_numbern]
```

To import FortiToken OTP seeds

```
execute fortitoken import <seeds_file> <seeds_file_preshared_key>
```

To synchronize a FortiToken device

```
execute fortitoken sync <serial_number> <code> <next code>
```

fortitoken-mobile

Use these commands to activate and synchronize a FortiToken Mobile card. FortiToken Mobile cards are used in two-factor authentication of administrator and user account logons. The FortiGate unit sends a random six-digit code to the mobile device by email or SMS that the user enters during the logon process along with user name and password.

Syntax

To import the FortiToken Mobile card serial number

```
execute fortitoken-mobile import <activation_code>
```

To poll a FortiToken Mobile token state

```
execute fortitoken-mobile poll
```

To provision a FortiToken Mobile token

```
execute fortitoken-mobile provision <token_serial_number>
```


fssso refresh

Use this command to manually refresh user group information from Directory Service servers connected to the FortiGate unit using the Fortinet Single Sign On (FSSO) agent.

Syntax

```
execute fssso refresh
```

ha disconnect

Use this command to disconnect a FortiGate unit from a functioning cluster. You must specify the serial number of the unit to be disconnected. You must also specify an interface name and assign an IP address and netmask to this interface of the disconnected unit. You can disconnect any unit from the cluster even the primary unit. After the unit is disconnected the cluster responds as if the disconnected unit has failed. The cluster may renegotiate and may select a new primary unit.

To disconnect the unit from the cluster, the `execute ha disconnect` command sets the HA mode of the disconnected unit to standalone. In addition, all interface IP addresses of the disconnected unit are set to 0.0.0.0. The interface specified in the command is set to the IP address and netmask that you specify in the command. In addition all management access to this interface is enabled. Once the FortiGate unit is disconnected you can use SSH, telnet, HTTPS, or HTTP to connect to and manage the FortiGate unit.

Syntax

```
execute ha disconnect <cluster-member-serial_str> <interface_str>  
                    <address_ipv4> <address_ipv4mask>
```

| Variable | Description |
|---------------------------|---|
| cluster-member-serial_str | The serial number of the cluster unit to be disconnected. |
| interface_str | The name of the interface to configure. The command configures the IP address and netmask for this interface and also enables all management access for this interface. |

Example

This example shows how to disconnect a cluster unit with serial number FGT5002803033050. The internal interface of the disconnected unit is set to IP address 1.1.1.1 and netmask 255.255.255.0.

```
execute ha disconnect FGT5002803033050 internal 1.1.1.1 255.255.255.0
```

ha ignore-hardware-revision

Use this command to set ignore-hardware-revision status.

Syntax

To view ignore-hardware-revision status

```
execute ha ignore-hardware-revision status
```

To set ignore-hardware-revision status

```
execute ha ignore-hardware-revision {enable | disable}
```

ha manage

Use this command from the CLI of a FortiGate unit in an HA cluster to log into the CLI of another unit in the cluster. Usually you would use this command from the CLI of the primary unit to log into the CLI of a subordinate unit. However, if you have logged into a subordinate unit CLI, you can use this command to log into the primary unit CLI, or the CLI of another subordinate unit.

You can use CLI commands to manage the cluster unit that you have logged into. If you make changes to the configuration of any cluster unit (primary or subordinate unit) these changes are synchronized to all cluster units.

Syntax

```
execute ha manage <cluster-index>
```

| Variable | Description |
|---------------|---|
| cluster-index | The cluster index is assigned by the FortiGate Clustering Protocol according to cluster unit serial number. The cluster unit with the highest serial number has a cluster index of 0. The cluster unit with the second highest serial number has a cluster index of 1 and so on. Enter ? to list the cluster indexes of the cluster units that you can log into. The list does not show the unit that you are already logged into. |

Example

This example shows how to log into a subordinate unit in a cluster of three FortiGate units. In this example you have already logged into the primary unit. The primary unit has serial number FGT3082103000056. The subordinate units have serial numbers FGT3012803021709 and FGT3082103021989.

```
execute ha manage ?
<id>    please input slave cluster index.
<0>     Subsidiary unit FGT3012803021709
<1>     Subsidiary unit FGT3082103021989
```

Type 0 and press enter to connect to the subordinate unit with serial number FGT3012803021709. The CLI prompt changes to the host name of this unit. To return to the primary unit, type `exit`.

From the subordinate unit you can also use the `execute ha manage` command to log into the primary unit or into another subordinate unit. Enter the following command:

```
execute ha manage ?
<id>    please input slave cluster index.
<1>     Subsidiary unit FGT3082103021989
<2>     Subsidiary unit FGT3082103000056
```

Type 2 and press enter to log into the primary unit or type 1 and press enter to log into the other subordinate unit. The CLI prompt changes to the host name of this unit.

ha synchronize

Use this command from a subordinate unit in an HA cluster to manually synchronize its configuration with the primary unit or to stop a synchronization process that is in progress.

Syntax

```
execute ha synchronize {start | stop}
```

| Variable | Description |
|----------|---|
| start | Start synchronizing the cluster configuration. |
| stop | Stop the cluster from completing synchronizing its configuration. |

interface dhcpclient-renew

Renew the DHCP client for the specified DHCP interface and close the CLI session. If there is no DHCP connection on the specified port, there is no output.

Syntax

```
execute interface dhcpclient-renew <port>
```

Example

This is the output for renewing the DHCP client on port1 before the session closes:

```
# execute interface dhcpclient-renew port1
renewing dhcp lease on port1
```

interface pppoe-reconnect

Reconnect to the PPPoE service on the specified PPPoE interface and close the CLI session. If there is no PPPoE connection on the specified port, there is no output.

Syntax

```
execute interface pppoe-reconnect <port>
```

log client-reputation-report

Use these commands to control client-reputation log actions.

Syntax

To accept a host so that it has its own baselines

```
execute log client-reputation-report accept <policy-id> <host>
```

To clear all auto-profile data

```
execute log client-reputation-report clear
```

To ignore a host, removing it from the abnormal list

```
execute log client-reputation-report ignore <policy-id> <host>
```

To refresh the data of one option result

```
execute log client-reputation-report refresh <policy-id> <option>  
      <action>
```

- <option> is one of bandwidth, session, failconn, geo, or app
- <action> is one of data, baseline, or data_baseline (both data and baseline)

To get baseline/average information of one option

```
execute log client-reputation-report result baseline <policy-id>  
      <option>
```

- <option> is one of bandwidth, session, or failconn

To get hourly data of a host visiting a country or using an application

```
execute log client-reputation-report result details {hourly | total}  
      <policy-id> <option> <name> <host>
```

- <option> is geo or app
- <name> is the name of the country or application

To list abnormal hosts of one or all options

```
execute log client-reputation-report result list <policy-id> <option>
```

- <option> is geo, app, or all

To list periodical data of one host of one option

```
execute log client-reputation-report result period <policy-id>  
      <option> <host> <periods>
```

- <option> is one of bandwidth, session, failconn, geo, or app
- <periods> is number of periods to list

To list the top 10 abnormal hosts of one option

```
execute log client-reputation-report result top10 <policy-id>  
      <option>
```

- <option> is one of bandwidth, session, failconn, geo, or app

To run reports immediately

```
execute log client-reputation-report run <policy-id>
```


log convert-oldlogs

Use this command to convert old compact logs to the new format. This command is available only if you have upgraded from an earlier version of FortiOS and have old compact logs on your system.

Syntax

```
execute log convert-oldlogs
```

log delete-all

Use this command to clear all log entries in memory and current log files on hard disk. If your FortiGate unit has no hard disk, only log entries in system memory will be cleared. You will be prompted to confirm the command.

Syntax

```
execute log delete-all
```

log delete-oldlogs

Use this command to delete old compact logs. This command is available only if you have upgraded from an earlier version of FortiOS and have old compact logs on your system.

Syntax

```
execute log delete-oldlogs
```

log display

Use this command to display log messages that you have selected with the `execute log filter` command.

Syntax

```
execute log display
```

The console displays the first 10 log messages. To view more messages, run the command again. You can do this until you have seen all of the selected log messages. To restart viewing the list from the beginning, use the commands

```
execute log filter start-line 1  
execute log display
```

You can restore the log filters to their default values using the command

```
execute log filter reset
```

log filter

Use this command to select log messages for viewing or deletion. You can view one log category on one device at a time. Optionally, you can filter the messages to select only specified date ranges or severities of log messages. For traffic logs, you can filter log messages by source or destination IP address.

Commands are cumulative. If you omit a required variable, the command displays the current setting.

Use as many `execute log filter` commands as you need to define the log messages that you want to view.

```
execute log filter category <category_name>
execute log filter device {disk | memory}
execute log filter dump
execute log filter field <name>
execute log filter ha-member <unitsn_str>
execute log filter reset [all | field]
execute log filter rolled_number <number>
execute log filter start-line <line_number>
execute log filter view-lines <count>
```

| Variable | Description | Default |
|--------------------------|---|-------------|
| category <category_name> | Enter the type of log you want to select. To see a list of available categories, enter <code>execute log filter category</code> | event |
| device {disk memory} | Device where the logs are stored. | disk |
| dump | Display current filter settings. | No default. |
| field <name> | Press Enter to view the fields that are available for the associated category. Enter the fields you want, using commas to separate multiple fields. | No default. |
| ha-member <unitsn_str> | Select logs from the specified HA cluster member. Enter the serial number of the unit. | |
| reset [all field] | Execute this command to reset all filter settings. You can use field option to reset only filter field settings. | No default. |
| rolled_number <number> | Select logs from rolled log file. 0 selects current log file. | 0 |
| start-line <line_number> | Select logs starting at specified line number. | 1 |
| view-lines <count> | Set lines per view. Range: 5 to 1000 | 10 |

log fortianalyzer test-connectivity

Use this command to test the connection to the FortiAnalyzer unit. This command is available only when FortiAnalyzer is configured.

Syntax

```
execute log fortianalyzer test-connectivity
```

Example

When FortiAnalyzer is connected, the output looks like this:

```
FortiAnalyzer Host Name: FortiAnalyzer-800B
FortiGate Device ID: FG50B3G06500085
Registration: registered
Connection: allow
Disk Space (Used/Allocated): 468/1003 MB
Total Free Space: 467088 MB
Log: Tx & Rx
Report: Tx & Rx
Content Archive: Tx & Rx
Quarantine: Tx & Rx
```

When FortiAnalyzer is not connected, the output is: Connect Error

log list

You can view the list of current and rolled log files on the console. The list shows the file name, size and timestamp.

Syntax

```
execute log list <category>
```

To see a list of available categories, enter

```
execute log list
```

Example

The output looks like this:

| | | |
|--------|-------|---------------------------|
| elog | 8704 | Fri March 6 14:24:35 2009 |
| elog.1 | 1536 | Thu March 5 18:02:51 2009 |
| elog.2 | 35840 | Wed March 4 22:22:47 2009 |

At the end of the list, the total number of files in the category is displayed. For example:

```
501 event log file(s) found.
```

log rebuild-sqldb

Use this command to rebuild the SQL database from log files.

If run in the VDOM context, only this VDOM's SQL database is rebuilt. If run in the global context, the SQL database is rebuilt for all VDOMs.



If SQL logging is disabled, this command is unavailable.

Syntax

```
execute log rebuild-sqldb
```


log recreate-sqldb

Use this command to recreate SQL log database.



If SQL logging is disabled, this command is unavailable.

Syntax

```
execute log recreate-sqldb
```

log-report reset

Use this command to delete all logs, archives and user configured report templates.

Syntax

```
execute log-report reset
```

log roll

Use this command to roll all log files.

Syntax

```
execute log roll
```

log upload-progress

Use this command to display the progress of the latest log upload.

Syntax

```
execute log upload-progress
```

modem dial

Dial the modem.

The dial command dials the accounts configured in `config system modem` until it makes a connection or it has made the maximum configured number of redial attempts.

This command can be used if the modem is in Standalone mode.

Syntax

```
execute modem dial
```

modem hangup

Hang up the modem.

This command can be used if the modem is in Standalone mode.

Syntax

```
execute modem hangup
```

modem trigger

This command sends a signal to the modem daemon, which causes the state machine to re-evaluate its current state. If for some reason the modem should be connected but isn't, then it will trigger a redial. If the modem should not be connected but is, this command will cause the modem to disconnect.

Syntax

```
execute modem trigger
```

mrouter clear

Clear multicast routes, RP-sets, IGMP membership records or routing statistics.

Syntax

Clear IGMP memberships:

```
execute mrouter clear igmp-group {{<group-address>} <interface-  
name>}  
execute mrouter clear igmp-interface <interface-name>
```

Clear multicast routes:

```
execute mrouter clear <route-type> {<group-address>  
{<source-address>}}
```

Clear PIM-SM RP-sets learned from the bootstrap router (BSR):

```
execute mrouter clear sparse-mode-bsr
```

Clear statistics:

```
execute mrouter clear statistics {<group-address>  
{<source-address>}}
```

| Variable | Description |
|------------------|--|
| <interface-name> | Enter the name of the interface on which you want to clear IGMP memberships. |
| <group-address> | Optionally enter a group address to limit the command to a particular group. |
| <route-type> | Enter one of: <ul style="list-style-type: none">• dense-routes - clear only PIM dense routes• multicast-routes - clear all types of multicast routes• sparse-routes - clear only sparse routes |
| <source-address> | Optionally, enter a source address to limit the command to a particular source address. You must also specify group-address. |

netscan

Use this command to start and stop the network vulnerability scanner and perform related functions.

Syntax

```
execute netscan import
execute netscan list
execute netscan start scan
execute netscan status
execute netscan stop
```

| Variable | Description |
|------------|---|
| import | Import hosts discovered on the last asset discovery scan. |
| list | List the hosts discovered on the last asset discover scan. |
| start scan | Start configured vulnerability scan. |
| status | Display the status of the current network vulnerability scan. |
| stop | Stop the current network vulnerability scan. |

pbx

Use this command to view active channels and to delete, list or upload music files for when music is playing while a caller is on hold.

Syntax

```
execute pbx active-call <list>
execute pbx extension <list>
execute pbx ftgd-voice-pkg {sip-trunk}
execute pbx music-on-hold {delete | list | upload}
execute pbx prompt upload ftp <file.tgz> <ftp_server_address>[:port]
    [<username>] [password>]
execute pbx prompt upload tftp <file.tgz> <ftp_server_address>[:port]
    [<username>] [password>]
execute pbx prompt upload usb <file.tgz> <ftp_server_address>[:port]
    [<username>] [password>]
execute pbx restore-default-prompts
execute pbx sip-trunk list
```

| Variables | Description |
|--|---|
| active-call <list> | Enter to display a list of the active calls being processed by the FortiGate Voice unit. |
| extension <list> | Enter to display the status of all extensions with SIP phones that have connected to the FortiGate Voice unit. |
| ftgd-voice-pkg {sip-trunk} | Enter to retrieve FortiGuard voice package sip trunk information. |
| music-on-hold {delete list upload} | Enter to either delete, list or upload music on hold files. You can upload music on hold files using FTP, TFTP, or from a USB drive plugged into the FortiGate Voice unit. |
| prompt upload ftp <file.tgz> <ftp_server_address>[:port] [<username>] [password>] | Upload new pbx voice prompt files using FTP. The voice prompt files should be added to a tar file and zipped. This file would usually have the extension tgz. You must include the filename, FTP server address (domain name of IPv4 address) and if required the username and password for the server. |
| prompt upload tftp <file.tgz> <ftp_server_address>[:port] [<username>] [password>] | Upload new pbx voice prompt files using TFTP. The voice prompt files should be added to a tar file and zipped. This file would usually have the extension tgz. You must include the filename and TFTP server IP address. |
| prompt upload usb <file.tgz> <ftp_server_address>[:port] [<username>] [password>] | Upload new pbx voice prompt files from a USB drive plugged into the FortiGate Voice unit. The voice prompt files should be added to a tar file and zipped. This file would usually have the extension tgz. You must include the filename. |
| restore-default-prompts | Restore default English voicemail and other PBX system prompts. Use this command if you have changed the default prompts and want to restore the default settings. |
| sip-trunk list | Enter to display the status of all SIP trunks that have been added to the FortiGate Voice configuration. |

Example command output

Enter the following command to view active calls:

```
execute pbx active-call
```

| Call-From | Call-To | Durated |
|-----------|---------|----------|
| 6016 | 6006 | 00:00:46 |

Enter the following command to display the status of all extensions

```
execute pbx extension list
```

| Extension | Host | Dialplan |
|-----------|--------------|-----------------|
| 6052 | Unregister | company-default |
| 6051 | Unregister | company-default |
| 6050 | Unregister | company-default |
| 6022 | Unregister | company-default |
| 6021/6021 | 172.30.63.34 | company-default |
| 6020 | Unregister | company-default |

Enter the following command to display the status of all SIP trunks

```
execute pbx sip-trunk list
```

| Name | Host | Username | Account-Type | State |
|------------|--------------|-----------|--------------|-------|
| Provider_1 | 192.169.20.1 | +55555555 | Static | N/A |

ping

Send an ICMP echo request (ping) to test the network connection between the FortiGate unit and another network device.

Syntax

```
execute ping {<address_ipv4> | <host-name_str>}
```

<host-name_str> should be an IP address, or a fully qualified domain name.

Example

This example shows how to ping a host with the IP address 172.20.120.16.

```
#execute ping 172.20.120.16
```

```
PING 172.20.120.16 (172.20.120.16): 56 data bytes
64 bytes from 172.20.120.16: icmp_seq=0 ttl=128 time=0.5 ms
64 bytes from 172.20.120.16: icmp_seq=1 ttl=128 time=0.2 ms
64 bytes from 172.20.120.16: icmp_seq=2 ttl=128 time=0.2 ms
64 bytes from 172.20.120.16: icmp_seq=3 ttl=128 time=0.2 ms
64 bytes from 172.20.120.16: icmp_seq=4 ttl=128 time=0.2 ms
--- 172.20.120.16 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.5 ms
```

ping-options, ping6-options

Set ICMP echo request (ping) options to control the way ping tests the network connection between the FortiGate unit and another network device.

Syntax

```
execute ping-options data-size <bytes>
execute ping-options df-bit {yes | no}
execute ping-options pattern <2-byte_hex>
execute ping-options repeat-count <repeats>
execute ping-options source {auto | <source-intf_ip>}
execute ping-options timeout <seconds>
execute ping-options tos <service_type>
execute ping-options ttl <hops>
execute ping-options validate-reply {yes | no}
execute ping-options view-settings
```

| Variable | Description | Default |
|-------------------------------------|--|-------------|
| data-size <bytes> | Specify the datagram size in bytes. | 56 |
| df-bit {yes no} | Set df-bit to yes to prevent the ICMP packet from being fragmented. Set df-bit to no to allow the ICMP packet to be fragmented. | no |
| pattern <2-byte_hex> | Used to fill in the optional data buffer at the end of the ICMP packet. The size of the buffer is specified using the data_size parameter. This allows you to send out packets of different sizes for testing the effect of packet size on the connection. | No default. |
| repeat-count <repeats> | Specify how many times to repeat ping. | 5 |
| source {auto <source-intf_ip>} | Specify the FortiGate interface from which to send the ping. If you specify auto, the FortiGate unit selects the source address and interface based on the route to the <host-name_str> or <host_ip>. Specifying the IP address of a FortiGate interface tests connections to different network segments from the specified interface. | auto |
| timeout <seconds> | Specify, in seconds, how long to wait until ping times out. | 2 |
| tos <service_type> | Set the ToS (Type of Service) field in the packet header to provide an indication of the quality of service wanted. <ul style="list-style-type: none"> lowdelay = minimize delay throughput = maximize throughput reliability = maximize reliability lowcost = minimize cost | 0 |
| ttl <hops> | Specify the time to live. Time to live is the number of hops the ping packet should be allowed to make before being discarded or returned. | 64 |
| validate-reply {yes no} | Select yes to validate reply data. | no |
| view-settings | Display the current ping-option settings. | No default. |

Example

Use the following command to increase the number of pings sent.

```
execute ping-options repeat-count 10
```

Use the following command to send all pings from the FortiGate interface with IP address 192.168.10.23.

```
execute ping-options source 192.168.10.23
```

ping6

Send an ICMP echo request (ping) to test the network connection between the FortiGate unit and an IPv6 capable network device.

Syntax

```
execute ping6 {<address_ipv6> | <host-name_str>}
```

Example

This example shows how to ping a host with the IPv6 address 12AB:0:0:CD30:123:4567:89AB:CDEF.

```
execute ping6 12AB:0:0:CD30:123:4567:89AB:CDEF
```

policy-packet-capture delete-all

Use this command to delete captured packets.

Syntax

```
execute policy-packet-capture delete-all
```

You will be asked to confirm that you want delete the packets.

reboot

Restart the FortiGate unit.



Abruptly powering off your FortiGate unit may corrupt its configuration. Using the reboot and shutdown options here or in the web-based manager ensure proper shutdown procedures are followed to prevent any loss of configuration.

Syntax

```
execute reboot <comment "comment_string">
```

<comment "comment_string"> allows you to optionally add a message that will appear in the hard disk log indicating the reason for the reboot. If the message is more than one word it must be enclosed in quotes.

Example

This example shows the reboot command with a message included.

```
execute reboot comment "December monthly maintenance"
```

report

Use these commands to manage reports.

Syntax

To flash report caches:

```
execute report flash-cache
```

To recreate the report database:

```
execute report recreate-db
```

To generate a report:

```
execute report run [<layout_name>["start-time" "end-time"]]
```

The start and end times have the format yyyy-mm-dd hh:mm:ss

report-config reset

Use this command to reset report templates to the factory default. Logs are not deleted.



If SQL logging is disabled, this command is unavailable.

Syntax

```
execute report-config reset
```

restore

Use this command to

- restore the configuration from a file
- change the FortiGate firmware
- change the FortiGate backup firmware
- restore an IPS custom signature file

When virtual domain configuration is enabled (in `system global`, `vdom-admin` is enabled), the content of the backup file depends on the administrator account that created it.

- A backup of the system configuration from the super admin account contains the global settings and the settings for all of the VDOMs. Only the super admin account can restore the configuration from this file.
- A backup file from a regular administrator account contains the global settings and the settings for the VDOM to which the administrator belongs. Only a regular administrator account can restore the configuration from this file.

Syntax

```
execute restore ase ftp <filename_str> <server_ipv4[:port_int]
    | server_fqdn[:port_int]> [<username_str> <password_str>]
execute restore ase tftp <filename_str> <server_ipv4[:port_int]>
execute restore av ftp <filename_str> <server_ipv4[:port_int]
    | server_fqdn[:port_int]> [<username_str> <password_str>]
execute restore av tftp <filename_str> <server_ipv4[:port_int]>
execute restore config flash <revision>
execute restore config ftp <filename_str> <server_ipv4[:port_int]
    | server_fqdn[:port_int]> [<username_str> <password_str>]
    [<backup_password_str>]
execute restore config management-station {normal | template
    | script} <rev_int>
execute restore config tftp <filename_str> <server_ipv4>
    [<backup_password_str>]
execute restore config usb <filename_str> [<backup_password_str>]
execute restore config usb-mode [<backup_password_str>]
execute restore forticlient tftp <filename_str> <server_ipv4>
execute restore image flash <revision>
execute restore image ftp <filename_str> <server_ipv4[:port_int]
    | server_fqdn[:port_int]> [<username_str> <password_str>]
execute restore image management-station <version_int>
execute restore image tftp <filename_str> <server_ipv4>
execute restore image usb <filename_str>
execute restore ips ftp <filename_str> <server_ipv4[:port_int]
    | server_fqdn[:port_int]> [<username_str> <password_str>]
execute restore ips tftp <filename_str> <server_ipv4>
execute restore ipsuserdefsig ftp <filename_str> <server_ipv4[:
    port_int] | server_fqdn[:port_int]> [<username_str>
    <password_str>]
execute restore ipsuserdefsig tftp <filename_str> <server_ipv4>
```

```

execute restore secondary-image ftp <filename_str> <server_ipv4[:port_int] | server_fqdn[:port_int]> [<username_str> <password_str>]
execute restore secondary-image tftp <filename_str> <server_ipv4>
execute restore secondary-image usb <filename_str>
execute restore src-vis <src-vis-pkgfile>
execute restore vcm {ftp | tftp} <filename_str> <server_ipv4>
execute restore vmlicense {ftp | tftp} <filename_str> <server_ipv4>

```

| Variable | Description |
|--|--|
| ase ftp <filename_str> <server_ipv4[:port_int] server_fqdn[:port_int]> [<username_str> <password_str>] | Restore the antispam engine. Download the restore file from an FTP server. The user and password to access the FTP server are only necessary if the server requires them |
| ase tftp <filename_str> <server_ipv4[:port_int]> | Restore the antispam engine. Download the restore file from a TFTP server. |
| av ftp <filename_str> <server_ipv4[:port_int] server_fqdn[:port_int]> [<username_str> <password_str>] | Download the antivirus database file from an FTP server to the FortiGate unit. |
| av tftp <filename_str> <server_ipv4[:port_int]> | Download the antivirus database file from a TFTP server to the FortiGate unit. |
| config flash <revision> | Restore the specified revision of the system configuration from the flash disk. |
| config ftp <filename_str> <server_ipv4[:port_int] server_fqdn[:port_int]> [<username_str> <password_str>] [<backup_password_str>] | Restore the system configuration from an FTP server. The new configuration replaces the existing configuration, including administrator accounts and passwords. If the backup file was created with a password, you must specify the password. |
| config management-station {normal template script} <rev_int> | Restore the system configuration from the central management server. The new configuration replaces the existing configuration, including administrator accounts and passwords. rev_int is the revision number of the saved configuration to restore. Enter 0 for the most recent revision. |
| config tftp <filename_str> <server_ipv4> [<backup_password_str>] | Restore the system configuration from a file on a TFTP server. The new configuration replaces the existing configuration, including administrator accounts and passwords. If the backup file was created with a password, you must specify the password. |
| config usb <filename_str> [<backup_password_str>] | Restore the system configuration from a file on a USB disk. The new configuration replaces the existing configuration, including administrator accounts and passwords. If the backup file was created with a password, you must specify the password. |

| Variable | Description |
|---|---|
| config usb-mode [<backup_password_str>] | Restore the system configuration from a USB disk. The new configuration replaces the existing configuration, including administrator accounts and passwords. When the USB drive is removed, the FortiGate unit needs to reboot and revert to the unit's existing configuration. If the backup file was created with a password, you must specify the password. |
| forticlient tftp <filename_str> <server_ipv4> | Download the FortiClient image from a TFTP server to the FortiGate unit. The filename must have the format: FortiClientSetup_versionmajor.versionminor.build.exe. For example, FortiClientSetup.4.0.377.exe. |
| image flash <revision> | Restore specified firmware image from flash disk. |
| image ftp <filename_str> <server_ipv4[:port_int] server_fqdn[:port_int]> [<username_str> <password_str>] | Download a firmware image from an FTP server to the FortiGate unit. The FortiGate unit reboots, loading the new firmware. This command is not available in multiple VDOM mode. |
| image management-station <version_int> | Download a firmware image from the central management station. This is available if you have configured a FortiManager unit as a central management server. This is also available if your account with FortiGuard Analysis and Management Service allows you to upload firmware images. |
| image tftp <filename_str> <server_ipv4> | Download a firmware image from a TFTP server to the FortiGate unit. The FortiGate unit reboots, loading the new firmware. This command is not available in multiple VDOM mode. |
| image usb <filename_str> | Download a firmware image from a USB disk to the FortiGate unit. The FortiGate unit reboots, loading the new firmware. |
| ips ftp <filename_str> <server_ipv4[:port_int] server_fqdn[:port_int]> [<username_str> <password_str>] | Download the IPS database file from an FTP server to the FortiGate unit. |
| ips tftp <filename_str> <server_ipv4> | Download the IPS database file from a TFTP server to the FortiGate unit. |
| ipsuserdefsig ftp <filename_str> <server_ipv4[:port_int] server_fqdn[:port_int]> [<username_str> <password_str>] | Restore IPS custom signature file from an FTP server. The file will overwrite the existing IPS custom signature file. |
| ipsuserdefsig tftp <filename_str> <server_ipv4> | Restore an IPS custom signature file from a TFTP server. The file will overwrite the existing IPS custom signature file. |
| secondary-image ftp <filename_str> <server_ipv4[:port_int] server_fqdn[:port_int]> [<username_str> <password_str>] | Download a firmware image from an FTP server as the backup firmware of the FortiGate unit. Available on models that support backup firmware images. |

| Variable | Description |
|---|---|
| secondary-image tftp <filename_str> <server_ipv4> | Download a firmware image from a TFTP server as the backup firmware of the FortiGate unit. Available on models that support backup firmware images. |
| secondary-image usb <filename_str> | Download a firmware image from a USB disk as the backup firmware of the FortiGate unit. The unit restarts when the upload is complete. Available on models that support backup firmware images. |
| src-vis <src-vis-pkgfile> | Download source visibility signature package. |
| vcm {ftp tftp} <filename_str> <server_ipv4> | Restore VCM engine/plugin from an ftp or tftp server. |
| vmlicense {ftp tftp} <filename_str> <server_ipv4> | Restore VM license (VM version of product only). |

Example

This example shows how to upload a configuration file from a TFTP server to the FortiGate unit and restart the FortiGate unit with this configuration. The name of the configuration file on the TFTP server is `backupconfig`. The IP address of the TFTP server is `192.168.1.23`.

```
execute restore config tftp backupconfig 192.168.1.23
```

revision

Use these commands to manage configuration and firmware image files on the local disk.

Syntax

To delete a configuration file

```
execute revision delete config <revision>
```

To delete a firmware image file

```
execute revision delete image <revision>
```

To list the configuration files

```
execute revision list config
```

To delete a firmware image file

```
execute revision list image
```


router clear bfd session

Use this command to clear bi-directional forwarding session.

Syntax

```
execute router clear bfd session <src_ip> <dst_ip> <interface>
```

| Variable | Description |
|-------------|---|
| <src_ip> | Select the source IP address of the session. |
| <dst_ip> | Select the destination IP address of the session. |
| <interface> | Select the interface for the session. |

router clear bgp

Use this command to clear BGP peer connections.

Syntax

```
execute router clear bgp all [soft] [in | out]
execute router clear bgp as <as_number> [soft] [in | out]
execute router clear bgp dampening {ip_address | ip/netmask}
execute router clear bgp external {in prefix-filter} [soft] [in |
    out]
execute router clear bgp flap-statistics {ip_address | ip/netmask}
execute router clear bgp ip <ip_address> [soft] [in | out]
```

| Variable | Description |
|---|--|
| all | Clear all BGP peer connections. |
| as <as_number> | Clear BGP peer connections by AS number. |
| dampening {ip_address ip/netmask} | Clear route flap dampening information for peer or network. |
| external {in prefix-filter} | Clear all external peers. |
| ip <ip_address> | Clear BGP peer connections by IP address. |
| peer-group | Clear all members of a BGP peer-group. |
| [in out] | Optionally limit clear operation to inbound only or outbound only. |
| flap-statistics {ip_address ip/netmask} | Clear flap statistics for peer or network. |
| soft | Do a soft reset that changes the configuration but does not disturb existing sessions. |

router clear ospf process

Use this command to clear and restart the OSPF router.

Syntax

IPv4:

```
execute router clear ospf process
```

IPv6:

```
execute router clear ospf6 process
```

router restart

Use this command to restart the routing software.

Syntax

```
execute router restart
```

send-fds-statistics

Use this command to send an FDS statistics report now, without waiting for the FDS statistics report interval to expire.

Syntax

```
execute send-fds-statistics
```

set system session filter

Use these commands to define the session filter for `get system session` commands.

Syntax

To clear the filter settings

```
execute set system session filter clear  
    {all|dport|dst|duration|expire|policy|proto|sport|src|vd}
```

To specify destination port

```
execute set system session filter dport <port_range>
```

To specify destination IP address

```
execute set system session filter dst <ip_range>
```

To specify duration

```
execute set system session filter duration <duration_range>
```

To specify expiry

```
execute set system session filter expire <expire_range>
```

To list the filter settings

```
execute set system session filter list
```

To invert a filter setting

```
execute set system session filter negate  
    {dport|dst|duration|expire|policy|proto|sport|src|vd}
```

To specify firewall policy ID

```
execute set system session filter policy <policy_range>
```

To specify protocol

```
execute set system session filter proto <protocol_range>
```

To specify source port

```
execute set system session filter sport <port_range>
```

To specify source IP address

```
execute set system session filter src <ip_range>
```

To specify virtual domain

```
execute set system session filter vd <vdom_index>
```

| Variable | Description |
|------------------|---|
| <duration_range> | The start and end times, separated by a space. |
| <expire_range> | The start and end times, separated by a space. |
| <ip_range> | The start and end IP addresses, separated by a space. |
| <policy_range> | The start and end policy numbers, separated by a space. |
| <port_range> | The start and end port numbers, separated by a space. |

| Variable | Description |
|------------------|---|
| <protocol_range> | The start and end protocol numbers, separated by a space. |
| <vdom_index> | The VDOM index number. -1 means all VDOMs. |

set-next-reboot

Use this command to start the FortiGate unit with primary or secondary firmware after the next reboot. Available on models that can store two firmware images. By default, the FortiGate unit loads the firmware from the primary partition.

VDOM administrators do not have permission to run this command. It must be executed by a super administrator.

Syntax

```
execute set-next-reboot {primary | secondary}
```


sfp-mode-sgmii

Change the SFP mode for an NP2 card to SGMII. By default when an AMC card is inserted the SFP mode is set to SERDES mode by default.

If a configured NP2 card is removed and re-inserted, the SFP mode goes back to the default.

In these situations, the `sfpmode-sgmii` command will change the SFP mode from SERDES to SGMII for the interface specified.

Syntax

```
execute sfpmode-sgmii <interface>
```

<interface> is the NP2 interface where you are changing the SFP mode.

shutdown

Shut down the FortiGate unit now. You will be prompted to confirm this command.



Abruptly powering off your FortiGate unit may corrupt its configuration. Using the reboot and shutdown options here or in the web-based manager ensure proper shutdown procedures are followed to prevent any loss of configuration.

Syntax

```
execute shutdown [comment <comment_string>]
```

`comment` is optional but you can use it to add a message that will appear in the event log message that records the shutdown. The `comment` message of the does not appear on the Alert Message console. If the message is more than one word it must be enclosed in quotes.

Example

This example shows the reboot command with a message included.

```
execute shutdown comment "emergency facility shutdown"
```

An event log message similar to the following is recorded:

```
2009-09-08 11:12:31 critical admin 41986 ssh(172.20.120.11) shutdown
    User admin shutdown the device from ssh(172.20.120.11). The reason
    is 'emergency facility shutdown'
```

ssh

Use this command to establish an ssh session with another system.

Syntax

```
execute ssh <destination> [<port>]
```

<destination> - the destination in the form user@ip or user@host.

[<port>] - optional TCP port number

Example

```
execute ssh admin@172.20.120.122
```

To end an ssh session, type exit:

```
FGT-6028030112 # exit
```

```
Connection to 172.20.120.122 closed.
```

```
FGT-8002805000 #
```

sync-session

Use this command to force a session synchronization.

Syntax

```
execute sync-session
```

tac report

Use this command to create a debug report to send to Fortinet Support. Normally you would only use this command if requested to by Fortinet Support.

Syntax

```
execute tac report
```

telnet

Use telnet client. You can use this tool to test network connectivity.

Syntax

```
execute telnet <telnet_ipv4>
```

<telnet_ipv4> is the address to connect with.

Type `exit` to close the telnet session.

time

Get or set the system time.

Syntax

```
execute time [<time_str>]
```

`time_str` has the form `hh:mm:ss`, where

- `hh` is the hour and can be 00 to 23
- `mm` is the minutes and can be 00 to 59
- `ss` is the seconds and can be 00 to 59

If you do not specify a time, the command returns the current system time.

You are allowed to shorten numbers to only one digit when setting the time. For example both 01:01:01 and 1:1:1 are allowed.

Example

This example sets the system time to 15:31:03:

```
execute time 15:31:03
```

traceroute

Test the connection between the FortiGate unit and another network device, and display information about the network hops between the device and the FortiGate unit.

Syntax

```
execute traceroute {<ip_address> | <host-name>}
```

Example

This example shows how to test the connection with <http://docs.forticare.com>. In this example the traceroute command times out after the first hop indicating a possible problem.

```
#execute traceoute docs.forticare.com
traceroute to docs.forticare.com (65.39.139.196), 30 hops max, 38 byte
  packets
 1  172.20.120.2 (172.20.120.2)  0.324 ms  0.427 ms  0.360 ms
 2  * * *
```

If your FortiGate unit is not connected to a working DNS server, you will not be able to connect to remote host-named locations with traceroute.

tracert6

Test the connection between the FortiGate unit and another network device using IPv6 protocol, and display information about the network hops between the device and the FortiGate unit.

Syntax

```
tracert6 [-Fdn] [-f first_ttl] [-i interface] [-m max_ttl]
[-s src_addr] [-q nprobes] [-w waittime] [-z sendwait]
host [paddatalen]
```

| Variable | Description |
|----------------|---|
| -F | Set Don't Fragment bit. |
| -d | Enable debugging. |
| -n | Do not resolve numeric address to domain name. |
| -f <first_ttl> | Set the initial time-to-live used in the first outgoing probe packet. |
| -i <interface> | Select interface to use for tracert. |
| -m <max_ttl> | Set the max time-to-live (max number of hops) used in outgoing probe packets. |
| -s <src_addr> | Set the source IP address to use in outgoing probe packets. |
| -q <nprobes> | Set the number probes per hop. |
| -w <waittime> | Set the time in seconds to wait for response to a probe. Default is 5. |
| -z <sendwait> | Set the time in milliseconds to pause between probes. |
| host | Enter the IP address or FQDN to probe. |
| <paddatalen> | Set the packet size to use when probing. |

update-ase

Use this command to manually initiate the antispam engine and rules update.

Syntax

```
execute update-ase
```

update-av

Use this command to manually initiate the virus definitions and engines update. To update both virus and attack definitions, use the `execute update-now` command.

Syntax

```
execute update-av
```

update-geo-ip

Use this command to obtain an update to the IP geography database from FortiGuard.

Syntax

```
execute update-geo-ip
```

update-ips

Use this command to manually initiate the Intrusion Prevention System (IPS) attack definitions and engine update. To update both virus and attack definitions, use the `execute update-now` command.

Syntax

```
execute update-ips
```

update-now

Use this command to manually initiate both virus and attack definitions and engine updates. To initiate only virus or attack definitions, use the `execute update-av` or `execute update-ids` command respectively.

Syntax

```
execute update-now
```

update-src-vis

Use this command to trigger an FDS update of the source visibility signature package.

Syntax

```
execute update-src-vis
```

upd-vd-license

Use this command to enter a Virtual Domain (VDOM) license key.

If you have a FortiGate- unit that supports VDOM licenses, you can purchase a license key from Fortinet to increase the maximum number of VDOMs to 25, 50, 100 or 500. By default, FortiGate units support a maximum of 10 VDOMs.

Available on FortiGate models that can be licensed for more than 10 VDOMs.

Syntax

```
execute upd-vd-license <license_key>
```

| Variable | Description |
|---------------|---|
| <license_key> | The license key is a 32-character string supplied by Fortinet. Fortinet requires your unit serial number to generate the license key. |

upload

Use this command to upload system configurations and firmware images to the flash disk from FTP, TFTP, or USB sources.

Syntax

To upload configuration files:

```
execute upload config ftp <filename_str> <comment> <server_ipv4[:  
    port_int] | server_fqdn[:port_int]> [<username_str>  
    [<password_str>]] [<backup_password_str>]  
execute upload config tftp <filename_str> <comment> <server_ipv4>  
execute upload config usb <filename_str> <comment>
```

To upload firmware image files:

```
execute upload image ftp <filename_str> <comment> <server_ipv4[:  
    port_int] | server_fqdn[:port_int]> [<username_str>  
    [<password_str>]]  
execute upload image tftp <filename_str> <comment> <server_ipv4>  
execute upload image usb <filename_str> <comment>
```

To upload report image files:

```
execute upload report-img ftp <filename_str> <server_ipv4[:port_int]  
    | server_fqdn[:port_int]> [<username_str> [<password_str>]]  
execute upload report-img tftp <filename_str> <server_ipv4>
```

| Variable | Description |
|--------------------------|---|
| <comment> | Comment string. |
| <filename_str> | Filename to upload. |
| <server_fqdn[:port_int]> | Server fully qualified domain name and optional port. |
| <server_ipv4[:port_int]> | Server IP address and optional port number. |
| <username_str> | Username required on server. |
| <password_str> | Password required on server. |
| <backup_password_str> | Password for backup file. |

usb-device

Use these commands to manage FortiExplorer IOS devices.

Syntax

List connected FortiExplorer IOS devices

```
execute usb-device list
```

Disconnect FortiExplorer IOS devices

```
execute usb-device disconnect
```

usb-disk

Use these commands to manage your USB disks.

Syntax

```
execute usb-disk delete <filename>
execute usb-disk format
execute usb-disk list
execute usb-disk rename <old_name> <new_name>
```

| Variable | Description |
|------------------------------|--|
| delete <filename> | Delete the named file from the USB disk. |
| format | Format the USB disk. |
| list | List the files on the USB disk. |
| rename <old_name> <new_name> | Rename a file on the USB disk. |

vpn certificate ca

Use this command to import a CA certificate from a TFTP or SCEP server to the FortiGate unit, or to export a CA certificate from the FortiGate unit to a TFTP server.

Before using this command you must obtain a CA certificate issued by a CA.

Digital certificates are used to ensure that both participants in an IPSec communications session are trustworthy, prior to an encrypted VPN tunnel being set up between the participants. The CA certificate is the certificate that the FortiGate unit uses to authenticate itself to other devices.



VPN peers must use digital certificates that adhere to the X.509 standard.

Digital certificates are not required for configuring FortiGate VPNs. Digital certificates are an advanced feature provided for the convenience of system administrators. This manual assumes the user has prior knowledge of how to configure digital certificates for their implementation.

Syntax

```
execute vpn certificate ca export tftp <certificate-name_str>
    <file-name_str> <tftp_ip>
execute vpn certificate ca import auto <ca_server_url>
    <ca_identifier_str>
execute vpn certificate ca import tftp <file-name_str> <tftp_ip>
```

| Variable | Description |
|------------------------|--|
| import | Import the CA certificate from a TFTP server to the FortiGate unit. |
| export | Export or copy the CA certificate from the FortiGate unit to a file on the TFTP server. Type ? for a list of certificates. |
| <certificate-name_str> | Enter the name of the CA certificate. |
| <file-name_str> | Enter the file name on the TFTP server. |
| <tftp_ip> | Enter the TFTP server address. |
| auto | Retrieve a CA certificate from a SCEP server. |
| tftp | Import the CA certificate to the FortiGate unit from a file on a TFTP server (local administrator PC). |
| <ca_server_url> | Enter the URL of the CA certificate server. |
| <ca_identifier_str> | CA identifier on CA certificate server (optional). |

Examples

Use the following command to import the CA certificate named `trust_ca` to the FortiGate unit from a TFTP server with the address `192.168.21.54`.

```
execute vpn certificate ca import trust_ca 192.168.21.54
```

vpn certificate crl

Use this command to get a CRL via LDAP, HTTP, or SCEP protocol, depending on the auto-update configuration.

In order to use the command `execute vpn certificate crl`, the authentication servers must already be configured.

Digital certificates are used to ensure that both participants in an IPSec communications session are trustworthy, prior to an encrypted VPN tunnel being set up between the participants. The CA certificate is the certificate that the FortiGate unit uses to authenticate itself to other devices.



VPN peers must use digital certificates that adhere to the X.509 standard.

Digital certificates are not required for configuring FortiGate VPNs. Digital certificates are an advanced feature provided for the convenience of system administrators. This manual assumes the user has prior knowledge of how to configure digital certificates for their implementation.

Syntax

```
execute vpn certificate crl import auto <crl-name>
```

| Variable | Description |
|------------|---|
| import | Import the CRL from the configured LDAP, HTTP, or SCEP authentication server to the FortiGate unit. |
| <crl-name> | Enter the name of the CRL. |
| auto | Trigger an auto-update of the CRL from the configured LDAP, HTTP, or SCEP authentication server. |

vpn certificate local

Use this command to generate a local certificate, to export a local certificate from the FortiGate unit to a TFTP server, and to import a local certificate from a TFTP server to the FortiGate unit.

Digital certificates are used to ensure that both participants in an IPSec communications session are trustworthy, prior to an encrypted VPN tunnel being set up between the participants. The local certificate is the certificate that the FortiGate unit uses to authenticate itself to other devices.

When you generate a certificate request, you create a private and public key pair for the local FortiGate unit. The public key accompanies the certificate request. The private key remains confidential.

When you receive the signed certificate from the CA, use the `vpn certificate local` command to install it on the FortiGate unit.



VPN peers must use digital certificates that adhere to the X.509 standard.

Digital certificates are not required for configuring FortiGate VPNs. Digital certificates are an advanced feature provided for the convenience of system administrators. This manual assumes the user has prior knowledge of how to configure digital certificates for their implementation.

Syntax - generate

```
execute vpn certificate local generate <certificate-name_str>
    <key-length> {<host_ip> | <domain-name_str> | email-addr_str}>
    [<optional_information>]
```

| Variable | Description |
|---|---|
| <certificate-name_str> | Enter a name for the certificate. The name can contain numbers (0-9), uppercase and lowercase letters (A-Z, a-z), and the special characters - and _. Other special characters and spaces are not allowed. |
| <host_ip> | |
| {<host_ip> <domain-name_str> email-addr_str>} | <p>Enter the host IP address (<code>host_ip</code>), the domain name (<code>domain-name_str</code>), or an email address (<code>email-addr_str</code>) to identify the FortiGate unit being certified. Preferably use an IP address or domain name. If this is impossible (such as with a dialup client), use an e-mail address.</p> <p>For <code>host_ip</code>, enter the IP address of the FortiGate unit.</p> <p>For <code>domain-name_str</code>, enter the fully qualified domain name of the FortiGate unit.</p> <p>For <code>email-addr_str</code>, enter an email address that identifies the FortiGate unit.</p> <p>If you specify a host IP or domain name, use the IP address or domain name associated with the interface on which IKE negotiations will take place (usually the external interface of the local FortiGate unit). If the IP address in the certificate does not match the IP address of this interface (or if the domain name in the certificate does not match a DNS query of the FortiGate unit's IP), then some implementations of IKE may reject the connection. Enforcement of this rule varies for different IPSec products.</p> |

| Variable | Description |
|--------------------------|--|
| <key-length> | Enter 1024, 1536 or 2048 for the size in bits of the encryption key. |
| [<optional_information>] | Enter optional_information as required to further identify the certificate. See “Optional information variables” on page 1007 for the list of optional information variables. You must enter the optional variables in order that they are listed in the table. To enter any optional variable you must enter all of the variables that come before it in the list. For example, to enter the organization_name_str, you must first enter the country_code_str, state_name_str, and city_name_str. While entering optional variables, you can type ? for help on the next required variable. |

Optional information variables

| Variable | Description |
|------------------------------|---|
| <country_code_str> | Enter the two-character country code. Enter <code>execute vpn certificates local generate <name_str> country</code> followed by a ? for a list of country codes. The country code is case sensitive. Enter <code>null</code> if you do not want to specify a country. |
| <state_name_str> | Enter the name of the state or province where the FortiGate unit is located. |
| <city_name_str> | Enter the name of the city, or town, where the person or organization certifying the FortiGate unit resides. |
| <organization-name_str> | Enter the name of the organization that is requesting the certificate for the FortiGate unit. |
| <organization-unit_name_str> | Enter a name that identifies the department or unit within the organization that is requesting the certificate for the FortiGate unit. |
| <email_address_str> | Enter a contact e-mail address for the FortiGate unit. |
| <ca_server_url> | Enter the URL of the CA (SCEP) certificate server that allows auto-signing of the request. |
| <challenge_password> | Enter the challenge password for the SCEP certificate server. |

Example - generate

Use the following command to generate a local certificate request with the name `branch_cert`, the domain name `www.example.com` and a key size of 1536.

```
execute vpn certificate local generate branch_cert 1536
www.example.com
```

Syntax - import/export

```
execute vpn certificate local import tftp <file-name_str> <tftp_ip>
execute vpn certificate local export tftp <certificate-name_str>
<file-name_str> <tftp_ip>
```

| Variable | Description |
|------------------------|---|
| import | Import the local certificate from a TFTP server to the FortiGate unit. |
| export | Export or copy the local certificate from the FortiGate unit to a file on the TFTP server. Type ? for a list of certificates. |
| <certificate-name_str> | Enter the name of the local certificate. |
| <tftp_ip> | Enter the TFTP server address. |
| <file-name_str> | Enter the file name on the TFTP server. |
| list | List local certificates. |

Examples - import/export

Use the following command to export the local certificate request generated in the above example from the FortiGate unit to a TFTP server. The example uses the file name `testcert` for the downloaded file and the TFTP server address `192.168.21.54`.

```
execute vpn certificate local export branch_cert testcert
192.168.21.54
```

Use the following command to import the signed local certificate named `branch_cert` to the FortiGate unit from a TFTP server with the address `192.168.21.54`.

```
execute vpn certificate local import branch_cert 192.168.21.54
```


vpn certificate remote

Use this command to import a remote certificate from a TFTP server, or export a remote certificate from the FortiGate unit to a TFTP server. The remote certificates are public certificates without a private key. They are used as OCSP (Online Certificate Status Protocol) server certificates.

Syntax

```
execute vpn certificate remote import tftp <file-name_str> <tftp_ip>  
execute vpn certificate remote export tftp <certificate-name_str>  
                                     <file-name_str> <tftp_ip>
```

| Field/variable | Description |
|------------------------|--|
| import | Import the remote certificate from the TFTP server to the FortiGate unit. |
| export | Export or copy the remote certificate from the FortiGate unit to a file on the TFTP server. Type ? for a list of certificates. |
| <certificate-name_str> | Enter the name of the public certificate. |
| <file-name_str> | Enter the file name on the TFTP server. |
| <tftp_ip> | Enter the TFTP server address. |
| tftp | Import/export the remote certificate via a TFTP server. |

vpn ipsec tunnel down

Use this command to shut down an IPsec VPN tunnel.

Syntax

```
execute vpn ipsec tunnel down <phase2> [<phase1> <phase2_serial>]
```

where:

- <phase2> is the phase 2 name
- <phase1> is the phase 1 name
- <phase2_serial> is the phase 2 serial number

<phase1> is required on a dial-up tunnel.

vpn ipsec tunnel up

Use this command to activate an IPsec VPN tunnel.

Syntax

```
execute vpn ipsec tunnel up <phase2> [<phase1> <phase2_serial>]
```

where:

- <phase2> is the phase 2 name
- <phase1> is the phase 1 name
- <phase2_serial> is the phase 2 serial number

This command cannot activate a dial-up tunnel.

vpn sslvpn del-all

Use this command to delete all SSL VPN connections in this VDOM.

Syntax

```
execute vpn sslvpn del-all
```

vpn sslvpn del-tunnel

Use this command to delete an SSL tunnel connection.

Syntax

```
execute vpn sslvpn del-tunnel <tunnel_index>
```

<tunnel_index> identifies which tunnel to delete if there is more than one active tunnel.

vpn sslvpn del-web

Use this command to delete an active SSL VPN web connection.

Syntax

```
execute vpn sslvpn del-web <web_index>
```

<web_index> identifies which web connection to delete if there is more than one active connection.

vpn sslvpn list

Use this command to list current SSL VPN tunnel connections.

Syntax

```
execute vpn sslvpn list {web | tunnel}
```

webfilter quota-reset

Use this command to reset user quota.

Syntax

```
execute webfilter quota-reset <wf-profile> <user_ip4addr>  
execute webfilter quota-reset <wf-profile> <user_name>
```


wireless-controller delete-wtp-image

Use this command to delete all firmware images for WLAN Termination Points (WTPs), also known as physical access points.

Syntax

```
execute wireless-controller delete-wtp-image
```

wireless-controller list-wtp-image

Use this command to list all firmware images for WLAN Termination Points (WTPs), also known as WiFi physical access points.

Syntax

```
execute wireless-controller list-wtp-image
```

Example output

WTP Images on AC:

| ImageName | ImageSize(B) | ImageInfo | ImageMTime |
|----------------|--------------|----------------------|-------------------------|
| FAP22A-IMG.wtp | 3711132 | FAP22A-v4.0-build212 | Mon Jun 6 12:26:41 2011 |

wireless-controller reset-wtp

Use this command to reset a physical access point (WTP).

If the FortiGate unit has a more recent version of the FortiAP firmware, the FortiAP unit will download and install it. Use the command [execute wireless-controller upload-wtp-image](#) to upload FortiAP firmware to the FortiGate unit.

Syntax

```
execute wireless-controller reset-wtp {<serialNumber_str> | all}
```

where <serialNumber_str> is the FortiWiFi unit serial number.

Use the `all` option to reset all APs.

wireless-controller restart-acd

Use this command to restart the wireless-controller daemon.

Syntax

```
execute wireless-controller restart-acd
```

wireless-controller restart-wtpd

Use this command to restart the wireless access point daemon.

Syntax

```
execute wireless-controller restart-wtpd
```

wireless-controller upload-wtp-image

Use this command to upload a FortiWiFi firmware image to the FortiGate unit. Wireless APs controlled by this wireless controller can download the image as needed. Use the [execute wireless-controller reset-wtp](#) command to trigger FortiAP units to update their firmware.

Syntax

FTP:

```
execute wireless-controller upload-wtp-image ftp <filename_str>  
      <server_ipv4[:port_int]> [<username_str> <password_str>]
```

TFTP:

```
execute wireless-controller upload-wtp-image tftp <filename_str>  
      <server_ipv4>
```



The `get` commands retrieve information about the operation and performance of your FortiGate unit.

This chapter contains the following sections:

| | | |
|---|--|---|
| endpoint-control app-detect | router info bfd neighbor | system interface physical |
| firewall dnstranslation | router info bgp | system mgmt-csum |
| firewall iprope appctrl | router info gwddetect | system performance firewall |
| firewall iprope list | router info isis | system performance status |
| firewall proute, proute6 | router info kernel | system performance top |
| firewall service custom | router info multicast | system session list |
| firewall shaper | router info ospf | system session status |
| grep | router info protocols | system session-helper-info list |
| gui console status | router info rip | system session-info |
| gui topology status | router info routing-table | system source-ip |
| hardware cpu | router info vrrp | system startup-error-log |
| hardware memory | router info6 bgp | system status |
| hardware nic | router info6 interface | test |
| hardware npu | router info6 kernel | user adgrp |
| hardware status | router info6 ospf | vpn ike gateway |
| ips decoder status | router info6 protocols | vpn ipsec tunnel details |
| ips rule status | router info6 rip | vpn ipsec tunnel name |
| ips session | router info6 routing-table | vpn ipsec stats crypto |
| ipsec tunnel | system admin list | vpn ipsec stats tunnel |
| ips view-map | system admin status | vpn ssl monitor |
| mgmt-data status | system arp | vpn status l2tp |
| netscan settings | system auto-update | vpn status pptp |
| pbx branch-office | system central-management | vpn status ssl |
| pbx dialplan | system checksum | webfilter ftgd-statistics |
| pbx did | system cmdb status | webfilter status |
| pbx extension | system fortianalyzer-connectivity | wireless-controller rf-analysis |
| pbx ftgd-voice-pkg | system fortiguard-log-service status | wireless-controller scan |
| pbx global | system fortiguard-service status | wireless-controller status |
| pbx ringgrp | system ha-nonsync-csum | wireless-controller vap-status |
| pbx sip-trunk | system ha status | wireless-controller wlanlistlic |
| pbx voice-menu | system info admin ssh | wireless-controller wtp-status |
| report database schema | system info admin status | |

endpoint-control app-detect

Use this command to retrieve information about predefined application detection signatures for Endpoint NAC.

Syntax

```
get endpoint-control app-detect predefined-category status
get endpoint-control app-detect predefined-group status
get endpoint-control app-detect predefined-signature status
get endpoint-control app-detect predefined-vendor status
```

Example output (partial)

```
get endpoint-control app-detect predefined-category status
FG200A2907500558 # get endpoint-control app-detect predefined-category
status
name: "Anti-Malware Software"
id: 1
group: 1

name: "Authentication and Authorization"
id: 2
group: 1

name: "Encryption, PKI"
id: 3
group: 1

name: "Firewalls"
id: 4
group: 1

get endpoint-control app-detect predefined-group status
FG200A2907500558 # get endpoint-control app-detect predefined-group
status
name: "Security"
id: 1

name: "Multimedia"
id: 2

name: "Communication"
id: 3

name: "Critical Functions"
id: 4
```



```
get endpoint-control app-detect predefined-signature status
FG200A2907500558 # get endpoint-control app-detect predefined-signature
status
name: "Apache HTTP Server"
id: 256
category: 26
vendor: 149

name: "RealPlayer (32-bit)"
id: 1
category: 10
vendor: 68

name: "VisualSVN Server"
id: 257
category: 26
vendor: 162

name: "QQ2009"
id: 2
category: 14
vendor: 78

get endpoint-control app-detect predefined-vendor status
FG200A2907500558 # get endpoint-control app-detect predefined-vendor
status
name: "Access Remote PC (www.access-remote-pc.com)"
id: 3

name: "ACD Systems, Ltd."
id: 4

name: "Adobe Systems Incorporated"
id: 5

name: "Alen Soft"
id: 6
```

firewall dnstranslation

Use this command to display the firewall DNS translation table.

Syntax

```
get firewall dnstranslation
```

firewall iprope appctrl

Use this command to list all application control signatures added to an application control list and display a summary of the application control configuration.

Syntax

```
get firewall iprope appctrl {list | status}
```

Example output

In this example, the FortiGate unit includes one application control list that blocks the FTP application.

```
get firewall iprope appctrl list
app-list=app_list_1/2000 other-action=Pass
  app-id=15896      list-id=2000  action=Block
```

```
get firewall iprope appctrl status
appctrl table 3 list 1 app 1 shaper 0
```

firewall iprope list

Use this command to list all of the FortiGate unit iprope firewall policies. Optionally include a group number in hexadecimal format to display a single policy. Policies are listed in FortiOS format.

Syntax

```
get firewall iprope list [<group_number_hex>]
```

Example output

```
get firewall iprope list 0010000c

policy flag (8000000): pol_stats
flag2 (20): ep_block shapers: / per_ip=
imflag: sockport: 1011 action: redirect index: 0
schedule() group=0010000c av=00000000 au=00000000 host=0 split=00000000
chk_client_info=0x0 app_list=0 misc=0 grp_info=0 seq=0 hash=0
npu_sensor_id=0
    tunnel=
zone(1): 0 ->zone(1): 0
source(0):
dest(0):
source wildcard(0):
destination wildcard(0):
service(1):
    [6:0x8:1011/(0,65535)->(80,80)]
nat(0):
mms: 0 0
```

firewall proute, proute6

Use these commands to list policy routes.

Syntax

For IPv4 policy routes:

```
get firewall proute
```

For IPv6 policy routes:

```
get firewall proute6
```

Example output

```
get firewall proute
list route policy info(vf=root):
iff=5 src=1.1.1.0/255.255.255.0 tos=0x00 tos_mask=0x00
    dst=0.0.0.0/0.0.0.0 protocol=80 port=1:65535
    oif=3 gwy=1.2.3.4
```

firewall service custom

Use this command to view the list of custom services. If you do not specify a <service_name> the command lists all of the pre-defined services.

Syntax

```
get firewall service custom
```

This lists the services.

To view details about all services

```
config firewall service custom
show full-configuration
```

To view details about a specific service

This example lists the configuration for the ALL_TCP service:

```
config firewall service custom
edit ALL_TCP
show full-configuration
```

Example output

This is a partial output.

```
get firewall service custom
== [ ALL ]
name: ALL
== [ ALL_TCP ]
name: ALL_TCP
== [ ALL_UDP ]
name: ALL_UDP
== [ ALL_ICMP ]
name: ALL_ICMP
== [ ALL_ICMP6 ]
name: ALL_ICMP6
== [ GRE ]
name: GRE
== [ AH ]
name: AH
== [ ESP ]
name: ESP
== [ AOL ]
name: AOL
== [ BGP ]
name: BGP
== [ DHCP ]
name: DHCP
== [ DNS ]
name: DNS
== [ FINGER ]
name: FINGER
```

firewall shaper

Use these command to retrieve information about traffic shapers.

Syntax

To get information about per-ip traffic shapers

```
get firewall shaper per-ip
```

To get information about shared traffic shapers

```
get firewall shaper traffic-shaper
```

grep

In many cases the `get` and `show` (and `diagnose`) commands may produce a large amount of output. If you are looking for specific information in a large `get` or `show` command output you can use the `grep` command to filter the output to only display what you are looking for. The `grep` command is based on the standard UNIX `grep`, used for searching text output based on regular expressions.

Information about how to use `grep` and regular expressions is available from the Internet. For example, see <http://www.opengroup.org/onlinepubs/009695399/utilities/grep.html>.

Syntax

```
{get | show | diagnose} | grep <regular_expression>
```

Example output

Use the following command to display the MAC address of the FortiGate unit internal interface:

```
get hardware nic internal | grep Current_HWaddr
Current_HWaddr                00:09:0f:cb:c2:75
```

Use the following command to display all TCP sessions in the session list and include the session list line number in the output

```
get system session list | grep -n tcp
19:tcp      1110    10.31.101.10:1862 172.20.120.122:30670
           69.111.193.57:1469 -
27:tcp      3599    10.31.101.10:2061 -          10.31.101.100:22 -
38:tcp      3594    10.31.101.10:4780 172.20.120.122:49700
           172.20.120.100:445 -
43:tcp      3582    10.31.101.10:4398 172.20.120.122:49574
           24.200.188.171:48726 -
```

Use the following command to display all lines in HTTP replacement message commands that contain URL (upper or lower case):

```
show system replacemsg http | grep -i url
set buffer "<HTML><BODY>The page you requested has been blocked
because it contains a banned word. URL =
%%PROTOCOL%%URL%%</BODY></HTML>"
config system replacemsg http "url-block"
set buffer "<HTML><BODY>The URL you requested has been blocked.
URL = %%URL%%</BODY></HTML>"
config system replacemsg http "urlfilter-err"
.
.
.
```


gui console status

Display information about the CLI console.

Syntax

```
get gui console status
```

Example

The output looks like this:

Preferences:

User: admin

Colour scheme (RGB): text=FFFFFF, background=000000

Font: style=monospace, size=10pt

History buffer=50 lines, external input=disabled

gui topology status

Display information about the topology viewer database. The topology viewer is available only if the Topology widget has been added to a customized web-based manager menu layout.

Syntax

```
get gui topology status
```

Example output

Preferences:

```
Canvas dimensions (pixels): width=780, height=800
Colour scheme (RGB): canvas=12ff08, lines=bf0f00,
exterior=ddeeee
Background image: type=none, placement: x=0, y=0
Line style: thickness=2
```

Custom background image file: none

Topology element database:

```
__FortiGate__: x=260, y=340
Office: x=22, y=105
ISPnet: x=222, y=129
__Text__: x=77, y=112: "Ottawa"
__Text__: x=276, y=139: "Internet"
```

hardware cpu

Use this command to display detailed information about all of the CPUs in your FortiGate unit.

Syntax

```
get hardware cpu
```

Example output

```
get hardware npu legacy list
No npu ports are found
```

```
620_ha_1 # get hardware cpu
processor          : 0
vendor_id         : GenuineIntel
cpu family        : 6
model             : 15
model name        : Intel(R) Core(TM)2 Duo CPU      E4300   @ 1.80GHz
stepping          : 13
cpu MHz           : 1795.545
cache size        : 64 KB
fdiv_bug          : no
hlt_bug           : no
f00f_bug          : no
coma_bug          : no
fpu               : yes
fpu_exception     : yes
cpuid level       : 10
wp                : yes
flags              : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge
                   mca cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe
                   lm pni monitor ds_cpl tm2 est
bogomips          : 3578.26

processor          : 1
vendor_id         : GenuineIntel
cpu family        : 6
model             : 15
model name        : Intel(R) Core(TM)2 Duo CPU      E4300   @ 1.80GHz
stepping          : 13
cpu MHz           : 1795.545
cache size        : 64 KB
fdiv_bug          : no
hlt_bug           : no
f00f_bug          : no
coma_bug          : no
fpu               : yes
fpu_exception     : yes
cpuid level       : 10
```

```
wp                : yes
flags             : fpu vme de pse tsc msr pae mce cx8 apic sep mtrr pge
                  mca cmov pat pse36 clflush dts acpi mmx fxsr sse sse2 ss ht tm pbe
                  lm pn1 monitor ds_cpl tm2 est
bogomips          : 3578.26
```

hardware memory

Use this command to display information about FortiGate unit memory use including the total, used, and free memory.

Syntax

```
get hardware memory
```

Example output

```
get hardware memory
      total:      used:      free:  shared: buffers:  cached: shm:
Mem:  3703943168 348913664 3355029504          0  192512 139943936
      137314304
Swap:          0          0          0
MemTotal:      3617132 kB
MemFree:       3276396 kB
MemShared:          0 kB
Buffers:        188 kB
Cached:        136664 kB
SwapCached:          0 kB
Active:        22172 kB
Inactive:     114740 kB
HighTotal:    1703936 kB
HighFree:    1443712 kB
LowTotal:    1913196 kB
LowFree:    1832684 kB
SwapTotal:          0 kB
SwapFree:          0 kB
```

hardware nic

Use this command to display hardware and status information about each FortiGate interface. The hardware information includes details such as the driver name and version and chip revision. Status information includes transmitted and received packets, and different types of errors.

Syntax

```
get hardware nic <interface_name>
```

| Variable | Description |
|------------------|--|
| <interface_name> | A FortiGate interface name such as port1, wan1, internal, etc. |

Example output

```
get hardware nic port9
Chip_Model          FA2/ISCP1B-v3/256MB
FPGA_REV_TAG        06101916
Driver Name          iscp1a/b-DE
Driver Version       0.1
Driver Copyright     Fortinet Inc.
```

```
Link                down
Speed               N/A
Duplex              N/A
State               up
```

```
Rx_Packets          0
Tx_Packets           0
Rx_Bytes             0
Tx_Bytes             0
```

```
Current_HWaddr      00:09:0f:77:09:68
Permanent_HWaddr    00:09:0f:77:09:68
```

```
Frame_Received       0
Bad Frame Received    0
Tx Frame              0
Tx Frame Drop         0
Receive IP Error      0
FIFO Error            0
```

```
Small PktBuf Left    125
Normal PktBuf Left    1021
Jumbo PktBuf Left     253
NAT Anomaly           0
```

hardware npu

Use this command to display information about the network processor unit (NPU) hardware installed in a FortiGate unit. The NPUs can be built-in or on an installed AMC module.

Syntax

```
get hardware npu legacy {list | session <device_name_str> | setting
    <device_name_str>}
get hardware npu np1 {list | status}
get hardware npu np2 {list | performance <device_id_int> | status
    <device_id_int>}
get hardware npu np4 {list | status <device_id_int>}
get hardware npu sp {list | status}
```

Example output

```
get hardware npu np1 list
```

```
ID          Interface
0           port9 port10
```

```
get hardware npu np1 status
```

```
ISCP1A 10ee:0702
RX SW Done 0 MTP 0x00000000
desc_size  = 0x00001000 count    = 0x00000100
nxt_to_u   = 0x00000000 nxt_to_f = 0x00000000
Total Number of Interfaces: 2
Number of Interface In-Use: 2
Interface[0] Tx done: 0
desc_size  = 0x00004000 count    = 0x00000100
nxt_to_u   = 0x00000000 nxt_to_f = 0x00000000
TX timeout = 0x00000000 BD_empty = 0x00000000
HRx Packets= 0x00000000 HTXBytes = 0x00000000 HRXBytes = 0x00000000
Interface[1] Tx done: 0
desc_size  = 0x00004000 count    = 0x00000100
nxt_to_u   = 0x00000000 nxt_to_f = 0x00000000
TX timeout = 0x00000000 BD_empty = 0x00000000
HRx Packets= 0x00000000 HTXBytes = 0x00000000 HRXBytes = 0x00000000
NAT Information:
head       = 0x00000001 tail    = 00000001
ISCP1A Performance [Top]:
Nr_int    : 0x00000000    INTwoInd  : 0x00000000    RXwoDone  :
0x00000000
PKTTwoEnd : 0x00000000    PKTCSErr  : 0x00000000
PKTidErr  : 0x00000000    PHY0Int   : 0x00000000    PHY1INT   :
0x00000000
CSUMOFF   : 0x00000000    BADCSUM   : 0x00000000    MSGINT    :
0x00000000
IPSEC     : 0x00000000    IPSVLAN   : 0x00000000    SESMISS   :
0x00000000
TOTUP     : 0x00000000    RSVD MEMU : 0x00000010
```

```

MSG Performance:
QLEN: 0x00001000 (QW) HEAD: 0x00000000
Performance:
TOTMSG: 0x00000000 BADMSG: 0x00000000 TOUTMSG: 0x00000000 QUERY:
0x00000000
NULLTK: 0x00000000
NAT Performance: BYPASS (Enable) BLOCK (Disable)
IRQ : 00000001 QFTL : 00000000 DELF : 00000000 FFTL : 00000000
OVTH : 00000001 QRYF : 00000000 INSF : 00000000 INVC : 00000000
ALLO : 00000000 FREE : 00000000 ALLOF : 00000000 BPENTR: 00000000
BKENTR: 00000000
BPENTR: 00000000 PBKENTR: 00000000 NOOP : 00000000 THROT :
00000000 (0x002625a0)
SWITOT : 00000000 SWDTOT : 00000000 ITDB : 00000000 OTDB : 00000000
SPISES : 00000000 FLUSH : 00000000
APS (Disabled) information:
MODE: BOTH UDPATH 255 ICMPTH 255 APSFLAGS: 0x00000000
IPSEC Offload Status: 0x58077dcb

```

```
get hardware npu np2 list
```

```

ID      PORTS
--      -
0      amc-sw1/1
0      amc-sw1/2
0      amc-sw1/3
0      amc-sw1/4
ID      PORTS
--      -
1      amc-dw2/1
ID      PORTS
--      -
2      amc-dw2/2

```

```
get hardware npu np2 status 0
```

```
NP2 Status
```

```

ISCP2 f7750000 (Neighbor 00000000) 1a29:0703 256MB Base f8aad000 DBG
0x00000000
RX SW Done 0 MTP 0x0
desc_alloc = f7216000
desc_size = 0x2000 count = 0x100
nxt_to_u = 0x0 nxt_to_f = 0x0
Total Interfaces: 4 Total Ports: 4
Number of Interface In-Use: 4
Interface f7750100 netdev 81b1e000 0 Name amc-sw1-1
PHY: Attached
LB Mode 0 LB IDX 0/1 LB Ports: f7750694, 00000000, 00000000, 00000000

```



```
Port f7750694 Id 0 Status Down ictr 4
desc = 8128c000
desc_size = 0x00001000 count = 0x000000100
nxt_to_u = 0x00000000 nxt_to_f = 0x00000000
Intf f7750100
Interface f7750264 netdev 81b2cc00 1 Name amc-sw1-2
PHY: Attached
LB Mode 0 LB IDX 0/1 LB Ports: f7750748, 00000000, 00000000, 00000000
Port f7750748 Id 1 Status Down ictr 0
desc = 81287000
desc_size = 0x00001000 count = 0x000000100
nxt_to_u = 0x00000000 nxt_to_f = 0x00000000
Intf f7750264
Interface f77503c8 netdev 81b2c800 2 Name amc-sw1-3
PHY: Attached
LB Mode 0 LB IDX 0/1 LB Ports: f77507fc, 00000000, 00000000, 00000000
Port f77507fc Id 2 Status Down ictr 0
desc = 81286000
desc_size = 0x00001000 count = 0x000000100
nxt_to_u = 0x00000000 nxt_to_f = 0x00000000
Intf f77503c8
Interface f775052c netdev 81b2c400 3 Name amc-sw1-4
PHY: Attached
LB Mode 0 LB IDX 0/1 LB Ports: f77508b0, 00000000, 00000000, 00000000
Port f77508b0 Id 3 Status Down ictr 0
desc = 81281000
desc_size = 0x00001000 count = 0x000000100
nxt_to_u = 0x00000000 nxt_to_f = 0x00000000
Intf f775052c
NAT Information:
cmdq_qw = 0x2000 cmdq = 82160000
head = 0x1 tail = 0x1
APS (Enabled) information:
Session Install when TMM TSE OOE: Disable
Session Install when TMM TAE OOE: Disable
IPS anomaly check policy: Follow config
MSG Base = 82150000 QL = 0x1000 H = 0x0
```

hardware status

Report information about the FortiGate unit hardware including FortiASIC version, CPU type, amount of memory, flash drive size, hard disk size (if present), USB flash size (if present), network card chipset, and WiFi chipset (FortiWifi models). This information can be useful for troubleshooting, providing information about your FortiGate unit to Fortinet Support, or confirming the features that your FortiGate model supports.

Syntax

```
get hardware status
```

Example output

```
Model name: Fortigate-620B
ASIC version: CP6
ASIC SRAM: 64M
CPU: Intel(R) Core(TM)2 Duo CPU      E4300   @ 1.80GHz
RAM: 2020 MB
Compact Flash: 493 MB /dev/sda
Hard disk: 76618 MB /dev/sdb
USB Flash: not available
Network Card chipset: Broadcom 570x Tigon3 Ethernet Adapter
                  (rev.0x5784100)
```

ips decoder status

Displays all the port settings of all the IPS decoders.

Syntax

```
get ips decoder status
```

Example output

```
# get ips decoder status
decoder-name: "back_orifice"
```

```
decoder-name: "dns_decoder"
port_list: 53
```

```
decoder-name: "ftp_decoder"
port_list: 21
```

```
decoder-name: "http_decoder"
```

```
decoder-name: "im_decoder"
```

```
decoder-name: "imap_decoder"
port_list: 143
```

Ports are shown only for decoders with configurable port settings.

ips rule status

Displays current configuration information about IPS rules.

Syntax

```
get ips rule status
```

Example output

```
# get ips rule status
rule-name: "IP.Land"
rule-id: 12588
rev: 2.464
action: pass
status: disable
log: enable
log-packet: disable
severity: 3.high
service: All
location: server, client
os: All
application: All

rule-name: "IP.Loose.Src.Record.Route.Option"
rule-id: 12805
rev: 2.464
action: pass
status: disable
log: enable
log-packet: disable
severity: 2.medium
service: All
location: server, client
os: All
application: All
```

ips session

Displays current IPS session status.

Syntax

```
get ips session
```

Example output

```
get ips session
```

```
SYSTEM:
memory capacity      279969792
memory used          5861008
recent pps\bps       0\0K
session in-use       0
TCP:  in-use\active\total  0\0\0
UDP:  in-use\active\total  0\0\0
ICMP: in-use\active\total  0\0\0
```

ipsec tunnel

List the current IPsec VPN tunnels and their status.

Syntax

To view details of all IPsec tunnels:

```
get ipsec tunnel details
```

To list IPsec tunnels by name:

```
get ipsec tunnel name
```

To view a summary of IPsec tunnel information:

```
get ipsec tunnel summary
```

ips view-map

Use this command to view the policies examined by IPS. This is mainly used for debugging. If there is no ips view map, it means IPS is not used or enabled.

Syntax

```
get ips view-map <id>
```

Example output

```
id                : 1
id-policy-id      : 0
policy-id         : 2
vdom-id           : 0
which             : firewall
```

| Variable | Description |
|--------------|--|
| id | IPS policy ID |
| id-policy-id | Identity-based policy ID (0 means none) |
| policy-id | Policy ID |
| vdom-id | VDOM, identified by ID number |
| which | Type of policy id: firewall, firewall6, sniffer, sniffer6, interface, interface6 |

mgmt-data status

Use this command to display information additional to that provided by `get system status` or `get hardware status`.

Syntax

```
get mgmt-data status
```

Sample output

```
FG100D3G12801361 # get mgmt-data status
Model name: FortiGate-100D
CPU: 4
RAM: 1977 MB
disk_is_ssd_available: 0
is_logdisk_mounted: 1
is_support_log_on_boot_device: 1
is_rev_support_wanopt: 1
```


netscan settings

Use this command to display tcp and udp ports that are scanned by the current scan mode.

Syntax

```
get netscan settings
```

Example output

```
scan-mode : full
tcp-ports  : 1-65535
udp-ports  : 1-65535
```

pbx branch-office

Use this command to list the configured branch offices.

Syntax

```
get pbx branch-office
```

Example output

```
== [ Branch 15 ]  
name: Branch 15  
== [ Branch 12 ]  
name: Branch 12
```

pbx dialplan

Use this command to list the configured dial plans.

Syntax

```
get pbx dialplan
```

Example output

```
== [ company-default ]  
name: company-default  
== [ inbound ]  
name: inbound
```

pbx did

Use this command to list the configured direct inward dial (DID) numbers.

Syntax

```
get pbx did
```

Example output

```
== [ Operator ]  
name: Operator  
== [ Emergency ]  
name: Emergency
```

pbx extension

Use this command to list the configured extensions.

Syntax

```
get pbx extension
```

Example output

```
== [ 6555 ]  
extension: 6555  
== [ 6777 ]  
extension: 6777  
== [ 6111 ]  
extension: 6111
```

pbx ftgd-voice-pkg

Use this command to display the current FortiGate Voice service package status.

Syntax

```
get pbx ftgd-voice-pkg status
```

Example output

```
Status: Activated
Total 1 Packages:
Package Type: B, Credit Left: 50.00, Credit Used: 0.00,
Expiration Date: 2011-01-01 12:00:00

Total 1 Dids:
12345678901
Total 1 Efxs:
12345678902
Total 0 Tollfrees:
```

pbx global

Use this command to display the current global pbx settings.

Syntax

```
get pbx global
```

Example output

```
block-blacklist      : enable
country-area         : USA
country-code         : 1
efax-check-interval  : 5
extension-pattern    : 6XXX
fax-admin-email      : faxad@example.com
ftgd-voice-server    : service.fortivoice.com
local-area-code      : 408
max-voicemail        : 60
outgoing-prefix      : 9
ring-timeout         : 20
rtp-hold-timeout     : 0
rtp-timeout          : 60
voicemail-extension  : *97
```

pbx ringgrp

Use this command to display the currently configured ring groups.

Syntax

```
get pbx ringgrp
```

Example output

```
== [ 6001 ]  
name: 6001  
== [ 6002 ]  
name: 6002
```


pbx sip-trunk

Use this command to display the currently configured SIP trunks.

Syntax

```
get pbx sip-trunk
```

Example output

```
== [ __FtgdVoice_1 ]  
name: __FtgdVoice_1
```

pbx voice-menu

Use this command to display the current voice menu and recorder extension configuration.

Syntax

```
get pbx voice-menu
```

Example output

```
comment          : general
password         : *
press-0:
    ring-group    : 6001
    type          : ring-group
press-1:
    type          : voicemail
press-2:
    type          : directory
press-3:
    type          : none
press-4:
    type          : none
press-5:
    type          : none
press-6:
    type          : none
press-7:
    type          : none
press-8:
    type          : none
press-9:
    type          : none
recorder-exten   : *30
```

report database schema

Use this command to display the FortiGate SQL reporting database schema.

Syntax

```
get report database schema
```

router info bfd neighbor

Use this command to list state information about the neighbors in the bi-directional forwarding table.

Syntax

```
get router info bfd neighbour
```

router info bgp

Use this command to display information about the BGP configuration.

Syntax

```
get router info bgp <keyword>
```

| <keyword> | Description |
|--|--|
| cidr-only | Show all BGP routes having non-natural network masks. |
| community | Show all BGP routes having their COMMUNITY attribute set. |
| community-info | Show general information about the configured BGP communities, including the routes in each community and their associated network addresses. |
| community-list | Show all routes belonging to configured BGP community lists. |
| dampening {dampened-paths flap-statistics parameters} | Display information about dampening: <ul style="list-style-type: none"> Type <code>dampened-paths</code> to show all paths that have been suppressed due to flapping. Type <code>flap-statistics</code> to show flap statistics related to BGP routes. Type <code>parameters</code> to show the current dampening settings. |
| filter-list | Show all routes matching configured AS-path lists. |
| inconsistent-as | Show all routes associated with inconsistent autonomous systems of origin. |
| memory | Show the BGP memory table. |
| neighbors [<address_ipv4> <address_ipv4> advertised-routes <address_ipv4> received prefix-filter <address_ipv4> received-routes <address_ipv4> routes] | Show information about connections to TCP and BGP neighbors. |
| network [<address_ipv4mask>] | Show general information about the configured BGP networks, including their network addresses and associated prefixes. |
| network-longer-prefixes <address_ipv4mask> | Show general information about the BGP route that you specify (for example, 12.0.0.0/14) and any specific routes associated with the prefix. |
| paths | Show general information about BGP AS paths, including their associated network addresses. |
| prefix-list <name> | Show all routes matching configured prefix list <name>. |
| quote-regexp <regexp_str> | Enter the regular expression to compare to the AS_PATH attribute of BGP routes (for example, ^730\$) and enable the use of output modifiers (for example, include, exclude, and begin) to search the results. |
| regexp <regexp_str> | Enter the regular expression to compare to the AS_PATH attribute of BGP routes (for example, ^730\$). |

| <keyword> | Description |
|-----------|--|
| route-map | Show all routes matching configured route maps. |
| scan | Show information about next-hop route scanning, including the scan interval setting. |
| summary | Show information about BGP neighbor status. |

Example output

```
get router info bgp memory
```

| Memory type | | Alloc count | Alloc bytes |
|---------------------------|---|-------------|-------------|
| ===== | | ===== | ===== |
| BGP structure | : | 2 | 1408 |
| BGP VR structure | : | 2 | 104 |
| BGP global structure | : | 1 | 56 |
| BGP peer | : | 2 | 3440 |
| BGP as list master | : | 1 | 24 |
| Community list handler | : | 1 | 32 |
| BGP Damp Reuse List Array | : | 2 | 4096 |
| BGP table | : | 62 | 248 |
| ----- | | ----- | ----- |
| Temporary memory | : | 4223 | 96095 |
| Hash | : | 7 | 140 |
| Hash index | : | 7 | 28672 |
| Hash bucket | : | 11 | 132 |
| Thread master | : | 1 | 564 |
| Thread | : | 4 | 144 |
| Link list | : | 32 | 636 |
| Link list node | : | 24 | 288 |
| Show | : | 1 | 396 |
| Show page | : | 1 | 4108 |
| Show server | : | 1 | 36 |
| Prefix IPv4 | : | 10 | 80 |
| Route table | : | 4 | 32 |
| Route node | : | 63 | 2772 |
| Vector | : | 2180 | 26160 |
| Vector index | : | 2180 | 18284 |
| Host config | : | 1 | 2 |
| Message of The Day | : | 1 | 100 |
| IMI Client | : | 1 | 708 |
| VTY master | : | 1 | 20 |
| VTY if | : | 11 | 2640 |
| VTY connected | : | 5 | 140 |
| Message handler | : | 2 | 120 |
| NSM Client Handler | : | 1 | 12428 |
| NSM Client | : | 1 | 1268 |
| Host | : | 1 | 64 |
| Log information | : | 2 | 72 |
| Context | : | 1 | 232 |
| ----- | | ----- | ----- |

```
bgp proto specifc allocations :      9408 B
bgp generic allocations       :      196333 B
bgp total allocations         :      205741 B
```

router info gwdetect

Use this command to view the status of gateway detection.

Syntax

```
get router info gwdetect
```


router info isis

Use this command to display information about the FortiGate ISIS.

Syntax

```
get router info isis interface
get router info isis neighbor
get router info isis is-neighbor
get router info isis database
get router info isis route
get router info isis topology
```

router info kernel

Use this command to display the FortiGate kernel routing table. The kernel routing table displays information about all of the routes in the kernel.

Syntax

```
get router info kernel [<routing_type_int>]
```

router info multicast

Use this command to display information about a Protocol Independent Multicasting (PIM) configuration. Multicast routing is supported in the root virtual domain only.

Syntax

```
get router info multicast <keywords>
```

| <keywords> | Description |
|-----------------|--|
| igmp | <p>Show Internet Group Management Protocol (IGMP) membership information according to one of these qualifiers:</p> <ul style="list-style-type: none"> Type <code>groups</code> [{<interface-name> <group-address>}] to show IGMP information for the multicast group(s) associated with the specified interface or multicast group address. Type <code>groups-detail</code> [{<interface-name> <group-address>}] to show detailed IGMP information for the multicast group(s) associated with the specified interface or multicast group address. Type <code>interface</code> [<interface-name>] to show IGMP information for all multicast groups associated with the specified interface. |
| pim dense-mode | <p>Show information related to dense mode operation according to one of these qualifiers:</p> <ul style="list-style-type: none"> Type <code>interface</code> to show information about PIM-enabled interfaces. Type <code>interface-detail</code> to show detailed information about PIM-enabled interfaces. Type <code>neighbor</code> to show the current status of PIM neighbors. Type <code>neighbor-detail</code> to show detailed information about PIM neighbors. Type <code>next-hop</code> to show information about next-hop PIM routers. Type <code>table</code> [<group-address>] [<source-address>] to show the multicast routing table entries associated with the specified multicast group address and/or multicast source address. |
| pim sparse-mode | <p>Show information related to sparse mode operation according to one of these qualifiers:</p> <ul style="list-style-type: none"> Type <code>bsr-info</code> to show Boot Strap Router (BSR) information. Type <code>interface</code> to show information about PIM-enabled interfaces. Type <code>interface-detail</code> to show detailed information about PIM-enabled interfaces. Type <code>neighbor</code> to show the current status of PIM neighbors. Type <code>neighbor-detail</code> to show detailed information about PIM neighbors. Type <code>next-hop</code> to show information about next-hop PIM routers. Type <code>rp-mapping</code> to show Rendezvous Point (RP) information. Type <code>table</code> [<group-address>] [<source-address>] to show the multicast routing table entries associated with the specified multicast group address and/or multicast source address. |

| <keywords> | Description |
|--|---|
| table [<group-address>] [<source-address>] | Show the multicast routing table entries associated with the specified multicast group address and/or multicast source address. |
| table-count [<group-address>] [<source-address>] | Show statistics related to the specified multicast group address and/or multicast source address. |

router info ospf

Use this command to display information about the FortiGate OSPF configuration and/or the Link-State Advertisements (LSAs) that the FortiGate unit obtains and generates. An LSA identifies the interfaces of all OSPF-enabled routers in an area, and provides information that enables OSPF-enabled routers to select the shortest path to a destination.

Syntax

```
get router info ospf <keyword>
```

| <keyword> | | Description |
|------------------------------|----------------------------|---|
| border-routers | | Show OSPF routing table entries that have an Area Border Router (ABR) or Autonomous System Boundary Router (ASBR) as a destination. |
| database <qualifier> | | <p>Show information from the OSPF routing database according to the of these qualifiers.</p> <p>Some qualifiers require a <code>target</code> that can be one of the following values:</p> <ul style="list-style-type: none"> Type <code>adv_router <address_ipv4></code> to limit the information to LSAs originating from the router at the specified IP address. Type <code>self-originate <address_ipv4></code> to limit the information to LSAs originating from the FortiGate unit. |
| | adv-router <address_ipv4> | Type <code>adv-router <address_ipv4></code> to show ospf Advertising Router link states for the router at the given IP address. |
| | asbr-summary <target> | Type <code>asbr-summary</code> to show information about ASBR summary LSAs. |
| | brief | Type <code>brief</code> to show the number and type of LSAs associated with each OSPF area. |
| | external <target> | Type <code>external</code> to show information about external LSAs. |
| | max-age | Type <code>max-age</code> to show all LSAs in the MaxAge list. |
| | network <target> | Type <code>network</code> to show information about network LSAs. |
| | nssa-external <target> | Type <code>nssa-external</code> to show information about not-so-stubby external LSAs. |
| | opaque-area <address_ipv4> | Type <code>opaque-area <address_ipv4></code> to show information about opaque Type 10 (area-local) LSAs (see RFC 2370). |
| | opaque-as <address_ipv4> | Type <code>opaque-as <address_ipv4></code> to show information about opaque Type 11 LSAs (see RFC 2370), which are flooded throughout the AS. |
| | opaque-link <address_ipv4> | Type <code>opaque-link <address_ipv4></code> to show information about opaque Type 9 (link-local) LSAs (see RFC 2370). |
| | router <target> | Type <code>router</code> to show information about router LSAs. |
| | self-originate | Type <code>self-originate</code> to show self-originated LSAs. |
| | summary <target> | Type <code>summary</code> to show information about summary LSAs. |
| interface [<interface_name>] | | Show the status of one or all FortiGate interfaces and whether OSPF is enabled on those interfaces. |

| <keyword> | Description |
|--|---|
| neighbor [all <neighbor_id> detail detail all interface <address_ipv4>] | Show general information about OSPF neighbors, excluding down-status neighbors: <ul style="list-style-type: none">• Type <code>all</code> to show information about all neighbors, including down-status neighbors.• Type <code><neighbor_id></code> to show detailed information about the specified neighbor only.• Type <code>detail</code> to show detailed information about all neighbors, excluding down-status neighbors.• Type <code>detail all</code> to show detailed information about all neighbors, including down-status neighbors.• Type <code>interface <address_ipv4></code> to show neighbor information based on the FortiGate interface IP address that was used to establish the neighbor's relationship. |
| route | Show the OSPF routing table. |
| status | Show general information about the OSPF routing processes. |
| virtual-links | Show information about OSPF virtual links. |

router info protocols

Use this command to show the current states of active routing protocols. Inactive protocols are not displayed.

Syntax

```
get router info protocols
```

Routing Protocol is "rip"

```
Sending updates every 30 seconds with +/-50%
Timeout after 180 seconds, garbage collect after 120 seconds
Outgoing update filter list for all interface is not set
Incoming update filter list for all interface is not set
Default redistribution metric is 1
Redistributing:
Default version control: send version 2, receive version 2
  Interface          Send Recv   Key-chain
Routing for Networks:
Routing Information Sources:
  Gateway            Distance  Last Update  Bad Packets  Bad Routes
Distance: (default is 120)
```

Routing Protocol is "ospf 0"

```
Invalid after 0 seconds, hold down 0, flushed after 0
Outgoing update filter list for all interfaces is
Incoming update filter list for all interfaces is
Redistributing:
Routing for Networks:
Routing Information Sources: Gateway          Distance      Last Update
Distance: (default is 110) Address          Mask          Distance
List
```

Routing Protocol is "bgp 5"

```
IGP synchronization is disabled
Automatic route summarization is disabled
Default local-preference applied to incoming route is 100
Redistributing:
Neighbor(s):
Address AddressFamily FiltIn FiltOut DistIn DistOut RouteMapIn
RouteMapOut Weight
192.168.20.10 unicast
```

router info rip

Use this command to display information about the RIP configuration.

Syntax

```
get router info rip <keyword>
```

| <keyword> | Description |
|------------------------------|---|
| database | Show the entries in the RIP routing database. |
| interface [<interface_name>] | Show the status of the specified FortiGate unit interface <interface_name> and whether RIP is enabled. If interface is used alone it lists all the FortiGate unit interfaces and whether RIP is enabled on each. |

router info routing-table

Use this command to display the routes in the routing table.

Syntax

```
get router info routing-table <keyword>
```

| <keyword> | Description |
|------------------------------|--|
| all | Show all entries in the routing table. |
| bgp | Show the BGP routes in the routing table. |
| connected | Show the connected routes in the routing table. |
| database | Show the routing information database. |
| details [<address_ipv4mask>] | Show detailed information about a route in the routing table, including the next-hop routers, metrics, outgoing interfaces, and protocol-specific information. |
| ospf | Show the OSPF routes in the routing table. |
| rip | Show the RIP routes in the routing table. |
| static | Show the static routes in the routing table. |

router info vrrp

Use this command to display information about the VRRP configuration.

Syntax

```
get router info vrrp
```

Example output

```
Interface: port1, primary IP address: 9.1.1.2
VRID: 1
  vrip: 9.1.1.254, priority: 100, state: BACKUP
  adv_interval: 1, preempt: 1, start_time: 3
  vrdst: 0.0.0.0
```

router info6 bgp

Use this command to display information about the BGP IPv6 configuration.

Syntax

```
get router info6 bgp <keyword>
```

| <keyword> | Description |
|---|--|
| community | Show all BGP routes having their COMMUNITY attribute set. |
| community-list | Show all routes belonging to configured BGP community lists. |
| dampening { dampened-paths flap-statistics parameters } | Display information about dampening: <ul style="list-style-type: none"> Type <code>dampened-paths</code> to show all paths that have been suppressed due to flapping. Type <code>flap-statistics</code> to show flap statistics related to BGP routes. Type <code>parameters</code> to show the current dampening settings. |
| filter-list | Show all routes matching configured AS-path lists. |
| inconsistent-as | Show all routes associated with inconsistent autonomous systems of origin. |
| neighbors [<address_ipv6mask> | Show information about connections to TCP and BGP neighbors. |
| network [<address_ipv6mask>] | Show general information about the configured BGP networks, including their network addresses and associated prefixes. |
| network-longer-prefixes <address_ipv6mask> | Show general information about the BGP route that you specify (for example, 12.0.0.0/14) and any specific routes associated with the prefix. |
| paths | Show general information about BGP AS paths, including their associated network addresses. |
| prefix-list <name> | Show all routes matching configured prefix list <name>. |
| quote-regexp <regexp_str> | Enter the regular expression to compare to the AS_PATH attribute of BGP routes (for example, ^730\$) and enable the use of output modifiers (for example, include, exclude, and begin) to search the results. |
| regexp <regexp_str> | Enter the regular expression to compare to the AS_PATH attribute of BGP routes (for example, ^730\$). |
| route-map | Show all routes matching configured route maps. |
| summary | Show information about BGP neighbor status. |

router info6 interface

Use this command to display information about IPv6 interfaces.

Syntax

```
get router info6 interface <interface_name>
```

Example output

The command returns the status of the interface and the assigned IPv6 address.

```
dmz2                                [administratively down/down]  
2001:db8:85a3:8d3:1319:8a2e:370:7348  
fe80::209:fff:fe04:4cfd
```

router info6 kernel

Use this command to display the FortiGate kernel routing table. The kernel routing table displays information about all of the routes in the kernel.

Syntax

```
get router info6 kernel
```

router info6 ospf

Use this command to display information about the OSPF IPv6 configuration.

Syntax

```
get router info6 ospf
```

router info6 protocols

Use this command to display information about the configuration of all IPv6 dynamic routing protocols.

Syntax

```
get router info6 protocols
```

router info6 rip

Use this command to display information about the RIPng configuration.

Syntax

```
get router info6 rip
```


router info6 routing-table

Use this command to display the routes in the IPv6 routing table.

Syntax

```
get router info6 routing-table <item>
```

where <item> is one of the following:

| Variable | Description |
|-----------|---------------------------------------|
| <ipv6_ip> | Destination IPv6 address or prefix. |
| bgp | Show BGP routing table entries. |
| connected | Show connected routing table entries. |
| database | Show routing information base. |
| ospf | Show OSPF routing table entries. |
| rip | Show RIP routing table entries. |
| static | Show static routing table entries. |

system admin list

View a list of all the current administration sessions.

Syntax

```
get system admin list
```

Example output

```
# get system admin list
username local    device                                remote                                started
admin    sshv2    port1:172.20.120.148:22  172.20.120.16:4167  2006-08-
          09 12:24:20
admin    https    port1:172.20.120.148:443 172.20.120.161:56365 2006-08-
          09 12:24:20
admin    https    port1:172.20.120.148:443 172.20.120.16:4214  2006-08-
          09 12:25:29
```

| | |
|----------|--|
| username | Name of the admin account for this session |
| local | The protocol this session used to connect to the FortiGate unit. |
| device | The interface, IP address, and port used by this session to connect to the FortiGate unit. |
| remote | The IP address and port used by the originating computer to connect to the FortiGate unit. |
| started | The time the current session started. |

system admin status

View the status of the currently logged in admin and their session.

Syntax

```
get system admin status
```

Example

The output looks like this:

```
# get system admin status
username: admin
login local: sshv2
login device: port1:172.20.120.148:22
login remote: 172.20.120.16:4167
login vdom: root
login started: 2006-08-09 12:24:20
current time: 2006-08-09 12:32:12
```

| | |
|---------------|---|
| username | Name of the admin account currently logged in. |
| login local | The protocol used to start the current session. |
| login device | The login information from the FortiGate unit including interface, IP address, and port number. |
| login remote | The computer the user is logging in from including the IP address and port number. |
| login vdom | The virtual domain the admin is current logged into. |
| login started | The time the current session started. |
| current time | The current time of day on the FortiGate unit |

system arp

View the ARP table entries on the FortiGate unit.

This command is not available in multiple VDOM mode.

Syntax

```
get system arp
```

Example output

```
# get system arp
Address           Age (min)  Hardware Addr  Interface
172.20.120.16     0          00:0d:87:5c:ab:65 internal
172.20.120.138    0          00:08:9b:09:bb:01 internal
```

system auto-update

Use this command to display information about the status FortiGuard updates on the FortiGate unit.

Syntax

```
get system auto-update status
get system auto-update versions
```

Example output

```
get system auto-update status
FDN availability:  available at Thu Apr  1 08:22:58 2010

Push update:  disable
Scheduled update:  enable
                Update daily:   8:22
Virus definitions update:  enable
IPS definitions update:  enable
Server override:  disable
Push address override:  disable
Web proxy tunneling:  disable
```

system central-management

View information about the Central Management System configuration.

Syntax

```
get system central-management
```

Example

The output looks like this:

```
FG600B3908600705 # get system central-management
status                : enable
type                  : fortimanager
auto-backup           : disable
schedule-config-restore: enable
schedule-script-restore: enable
allow-push-configuration: enable
allow-pushd-firmware: enable
allow-remote-firmware-upgrade: enable
allow-monitor         : enable
fmg                   : 172.20.120.161
vdom                   : root
authorized-manager-only: enable
serial-number         : "FMG-3K2404400063"
```

system checksum

View the checksums for global, root, and all configurations. These checksums are used by HA to compare the configurations of each cluster unit.

Syntax

```
get system checksum status
```

Example output

```
# get system checksum status
global: 7a 87 3c 14 93 bc 98 92 b0 58 16 f2 eb bf a4 15
root:   bb a4 80 07 42 33 c2 ff f1 b5 6e fe e4 bb 45 fb
all:    1c 28 f1 06 fa 2e bc 1f ed bd 6b 21 f9 4b 12 88
```

system cmdb status

View information about cmdbsvr on the FortiGate unit. FortiManager uses some of this information.

Syntax

```
get system cmdb status
```

Example output

```
# get system cmdb status
version: 1
owner id: 18
update index: 6070
config checksum: 12879299049430971535
last request pid: 68
last request type: 29
last request: 78
```

| Variable | Description |
|-------------------|--|
| version | Version of the cmdb software. |
| owner id | Process ID of the cmdbsvr daemon. |
| update index | The updated index shows how many changes have been made in cmdb. |
| config checksum | The config file version used by FortiManager. |
| last request pid | The last process to access the cmdb. |
| last request type | Type of the last attempted access of cmdb. |
| last request | The number of the last attempted access of cmdb. |

system fortianalyzer-connectivity

Display connection and remote disk usage information about a connected FortiAnalyzer unit.

Syntax

```
get fortianalyzer-connectivity status
```

Example output

```
# get system fortianalyzer-connectivity status
Status: connected
Disk Usage: 0%
```

system fortiguard-log-service status

Command returns information about the status of the FortiGuard Log & Analysis Service including license and disk information.

Syntax

```
get system fortiguard-log-service status
```

Example output

```
# get system fortiguard-log-service status
FortiGuard Log & Analysis Service
Expire on: 20071231
Total disk quota: 1111 MB
Max daily volume: 111 MB
Current disk quota usage: n/a
```

system fortiguard-service status

COMMAND REPLACED. Command returns information about the status of the FortiGuard service including the name, version late update, method used for the last update and when the update expires. This information is shown for the AV Engine, virus definitions, attack definitions, and the IPS attack engine.

Syntax

```
get system fortiguard-service status
```

Example output

| NAME | VERSION | LAST UPDATE | METHOD | EXPIRE |
|--------------------|---------|---------------------|--------|---------------------|
| AV Engine | 2.002 | 2006-01-26 19:45:00 | manual | 2006-06-12 08:00:00 |
| Virus Definitions | 6.513 | 2006-06-02 22:01:00 | manual | 2006-06-12 08:00:00 |
| Attack Definitions | 2.299 | 2006-06-09 19:19:00 | manual | 2006-06-12 08:00:00 |
| IPS Attack Engine | 1.015 | 2006-05-09 23:29:00 | manual | 2006-06-12 08:00:00 |

system ha-nonsync-csum

FortiManager uses this command to obtain a system checksum.

Syntax

```
get system ha-nonsync-csum
```

system ha status

Use this command to display information about an HA cluster. The command displays general HA configuration settings. The command also displays information about how the cluster unit that you have logged into is operating in the cluster.

Usually you would log into the primary unit CLI using SSH or telnet. In this case the `get system ha status` command displays information about the primary unit first, and also displays the HA state of the primary unit (the primary unit operates in the work state). However, if you log into the primary unit and then use the `execute ha manage` command to log into a subordinate unit, (or if you use a console connection to log into a subordinate unit) the `get system status` command displays information about this subordinate unit first, and also displays the HA state of this subordinate unit. The state of a subordinate unit is work for an active-active cluster and standby for an active-passive cluster.

For a virtual cluster configuration, the `get system ha status` command displays information about how the cluster unit that you have logged into is operating in virtual cluster 1 and virtual cluster 2. For example, if you connect to the cluster unit that is the primary unit for virtual cluster 1 and the subordinate unit for virtual cluster 2, the output of the `get system ha status` command shows virtual cluster 1 in the work state and virtual cluster 2 in the standby state. The `get system ha status` command also displays additional information about virtual cluster 1 and virtual cluster 2.

Syntax

```
get system ha status
```

The command display includes the following fields. For more information see the examples that follow.

| Variable | Description |
|-----------------|---|
| Model | The FortiGate model number. |
| Mode | The HA mode of the cluster: a-a or a-p. |
| Group | The group ID of the cluster. |
| Debug | The debug status of the cluster. |
| ses_pickup | The status of session pickup: enable or disable. |
| load_balance | The status of the <code>load-balance-all</code> field: enable or disable. Displayed for active-active clusters only. |
| schedule | The active-active load balancing schedule. Displayed for active-active clusters only. |
| Master Slave | <p><code>Master</code> displays the device priority, host name, serial number, and actual cluster index of the primary (or master) unit.</p> <p><code>Slave</code> displays the device priority, host name, serial number, and actual cluster index of the subordinate (or slave, or backup) unit or units.</p> <p>The list of cluster units changes depending on how you log into the CLI. Usually you would use SSH or telnet to log into the primary unit CLI. In this case the primary unit would be at the top the list followed by the other cluster units.</p> <p>If you use <code>execute ha manage</code> or a console connection to log into a subordinate unit CLI, and then enter <code>get system ha status</code> the subordinate unit that you have logged into appears at the top of the list of cluster units.</p> |

| Variable | Description |
|--------------------|--|
| number of vcluster | The number of virtual clusters. If virtual domains are not enabled, the cluster has one virtual cluster. If virtual domains are enabled the cluster has two virtual clusters. |
| vcluster 1 | <p>The HA state (hello, work, or standby) and HA heartbeat IP address of the cluster unit that you have logged into in virtual cluster 1. If virtual domains are not enabled, <code>vcluster 1</code> displays information for the cluster. If virtual domains are enabled, <code>vcluster 1</code> displays information for virtual cluster 1.</p> <p>The HA heartbeat IP address is 10.0.0.1 if you are logged into a the primary unit of virtual cluster 1 and 10.0.0.2 if you are logged into a subordinate unit of virtual cluster 1.</p> <p><code>vcluster 1</code> also lists the primary unit (master) and subordinate units (slave) in virtual cluster 1. The list includes the operating cluster index and serial number of each cluster unit in virtual cluster 1. The cluster unit that you have logged into is at the top of the list.</p> <p>If virtual domains are not enabled and you connect to the primary unit CLI, the HA state of the cluster unit in virtual cluster 1 is work. The display lists the cluster units starting with the primary unit.</p> <p>If virtual domains are not enabled and you connect to a subordinate unit CLI, the HA state of the cluster unit in virtual cluster 1 is standby. The display lists the cluster units starting with the subordinate unit that you have logged into.</p> <p>If virtual domains are enabled and you connect to the virtual cluster 1 primary unit CLI, the HA state of the cluster unit in virtual cluster 1 is work. The display lists the cluster units starting with the virtual cluster 1 primary unit.</p> <p>If virtual domains are enabled and you connect to the virtual cluster 1 subordinate unit CLI, the HA state of the cluster unit in virtual cluster 1 is standby. The display lists the cluster units starting with the subordinate unit that you are logged into.</p> <p>In a cluster consisting of two cluster units operating without virtual domains enabled all clustering actually takes place in virtual cluster 1. HA is designed to work this way to support virtual clustering. If this cluster was operating with virtual domains enabled, adding virtual cluster 2 is similar to adding a new copy of virtual cluster 1. Virtual cluster 2 is visible in the <code>get system ha status</code> command output when you add virtual domains to virtual cluster 2.</p> |

| Variable | Description |
|------------|--|
| vcluster 2 | <p><code>vcluster 2</code> only appears if virtual domains are enabled. <code>vcluster 2</code> displays the HA state (hello, work, or standby) and HA heartbeat IP address of the cluster unit that you have logged into in virtual cluster 2. The HA heartbeat IP address is 10.0.0.2 if you are logged into the primary unit of virtual cluster 2 and 10.0.0.1 if you are logged into a subordinate unit of virtual cluster 2.</p> <p><code>vcluster 2</code> also lists the primary unit (master) and subordinate units (slave) in virtual cluster 2. The list includes the cluster index and serial number of each cluster unit in virtual cluster 2. The cluster unit that you have logged into is at the top of the list.</p> <p>If you connect to the virtual cluster 2 primary unit CLI, the HA state of the cluster unit in virtual cluster 2 is <code>work</code>. The display lists the cluster units starting with the virtual cluster 2 primary unit.</p> <p>If you connect to the virtual cluster 2 subordinate unit CLI, the HA state of the cluster unit in virtual cluster 2 is <code>standby</code>. The display lists the cluster units starting with the subordinate unit that you are logged into.</p> |

system info admin ssh

Use this command to display information about the SSH configuration on the FortiGate unit such as:

- the SSH port number
- the interfaces with SSH enabled
- the hostkey DSA fingerprint
- the hostkey RSA fingerprint

Syntax

```
get system info admin ssh
```

Example output

```
# get system info admin ssh
SSH v2 is enabled on port 22
SSH is enabled on the following 1 interfaces:
    internal
SSH hostkey DSA fingerprint = cd:e1:87:70:bb:f0:9c:7d:e3:7b:73:f7:44:
    23:a5:99
SSH hostkey RSA fingerprint = c9:5b:49:1d:7c:ba:be:f3:9d:39:33:4d:48:
    9d:b8:49
```


system info admin status

Use this command to display administrators that are logged into the FortiGate unit.

Syntax

```
get system info admin status
```

Example

This shows sample output.

| Index | User name | Login type | From |
|-------|-----------|------------|--------------------|
| 0 | admin | CLI | ssh(172.20.120.16) |
| 1 | admin | WEB | 172.20.120.16 |

| | |
|------------|--|
| Index | The order the administrators logged in. |
| User name | The name of the user account logged in. |
| Login type | Which interface was used to log in. |
| From | The IP address this user logged in from. |

Related topics

- [get system info admin ssh](#)

system interface physical

Use this command to list information about the unit's physical network interfaces.

Syntax

```
get system interface physical
```

The output looks like this:

```
# get system interface physical
== [onboard]
    == [dmz1]
        mode: static
        ip: 0.0.0.0 0.0.0.0
        status: down
        speed: n/a
    == [dmz2]
        mode: static
        ip: 0.0.0.0 0.0.0.0
        status: down
        speed: n/a
    == [internal]
        mode: static
        ip: 172.20.120.146 255.255.255.0
        status: up
        speed: 100
    == [wan1]
        mode: pppoe
        ip: 0.0.0.0 0.0.0.0
        status: down
        speed: n/a
    == [wan2]
        mode: static
        ip: 0.0.0.0 0.0.0.0
        status: down
        speed: n/a
    == [modem]
        mode: static
        ip: 0.0.0.0 0.0.0.0
        status: down
        speed: n/a
```

system mgmt-csum

FortiManager uses this command to obtain checksum information from FortiGate units.

Syntax

```
get system mgmt-csum {global | vdom | all}
```

where

global retrieves global object checksums

vdom retrieves VDOM object checksums

all retrieves all object checksums.

system performance firewall

Use this command to display packet distribution and traffic statistics information for the FortiGate firewall.

Syntax

```
get system performance firewall packet-distribution
get system performance firewall statistics
```

| Variable | Description |
|---------------------|--|
| packet-distribution | Display a list of packet size ranges and the number of packets of each size accepted by the firewall since the system restarted. You can use this information to learn about the packet size distribution on your network. |
| statistics | Display a list of traffic types (browsing, email, DNS etc) and the number of packets and number of payload bytes accepted by the firewall for each type since the FortiGate unit was restarted. |

Example output

```
get system performance firewall packet-distribution
getting packet distribution statistics...
0 bytes - 63 bytes: 655283 packets
64 bytes - 127 bytes: 1678278 packets
128 bytes - 255 bytes: 58823 packets
256 bytes - 383 bytes: 70432 packets
384 bytes - 511 bytes: 1610 packets
512 bytes - 767 bytes: 3238 packets
768 bytes - 1023 bytes: 7293 packets
1024 bytes - 1279 bytes: 18865 packets
1280 bytes - 1500 bytes: 58193 packets
> 1500 bytes: 0 packets

get system performance firewall statistics
getting traffic statistics...
Browsing: 623738 packets, 484357448 bytes
DNS: 5129187383836672 packets, 182703613804544 bytes
E-Mail: 23053606 packets, 2 bytes
FTP: 0 packets, 0 bytes
Gaming: 0 packets, 0 bytes
IM: 0 packets, 0 bytes
Newsgroups: 0 packets, 0 bytes
P2P: 0 packets, 0 bytes
Streaming: 0 packets, 0 bytes
TFTP: 654722117362778112 packets, 674223966126080 bytes
VoIP: 16834455 packets, 10 bytes
Generic TCP: 266287972352 packets, 8521215115264 bytes
Generic UDP: 0 packets, 0 bytes
Generic ICMP: 0 packets, 0 bytes
Generic IP: 0 packets, 0 bytes
```

system performance status

Use this command to display FortiGate CPU usage, memory usage, network usage, sessions, virus, IPS attacks, and system up time.

Syntax

```
get system performance status
```

| Variable | Description |
|-----------------------|--|
| CPU states | <p>The percentages of CPU cycles used by user, system, nice and idle categories of processes. These categories are:</p> <ul style="list-style-type: none">• <code>user</code> -CPU usage of normal user-space processes• <code>system</code> -CPU usage of kernel• <code>nice</code> - CPU usage of user-space processes having other-than-normal running priority• <code>idle</code> - Idle CPU cycles <p>Adding user, system, and nice produces the total CPU usage as seen on the CPU widget on the web-based system status dashboard.</p> |
| Memory states | The percentage of memory used. |
| Average network usage | The average amount of network traffic in kbps in the last 1, 10 and 30 minutes. |
| Average sessions | The average number of sessions connected to the FortiGate unit over the last 1, 10 and 30 minutes. |
| Virus caught | The number of viruses the FortiGate unit has caught in the last 1 minute. |
| IPS attacks blocked | The number of IPS attacks that have been blocked in the last 1 minute. |
| Uptime | How long since the FortiGate unit has been restarted. |

Example output

```
# get system performance status
CPU states: 0% user 0% system 0% nice 100% idle
Memory states: 18% used
Average network usage: 0 kbps in 1 minute, 0 kbps in 10 minutes, 1 kbps
in 30 minutes
Average sessions: 5 sessions in 1 minute, 6 sessions in 10 minutes, 5
sessions in 30 minutes
Virus caught: 0 total in 1 minute
IPS attacks blocked: 0 total in 1 minute
Uptime: 9days, 22 hours, 0 minutes
```

system performance top

Use this command to display the list of processes running on the FortiGate unit (similar to the Linux `top` command).

You can use the following commands when `get system performance top` is running:

- Press Q or Ctrl+C to quit.
- Press P to sort the processes by the amount of CPU that the processes are using.
- Press M to sort the processes by the amount of memory that the processes are using.

Syntax

```
get system performance top [<delay_int>] <max_lines_int>]]
```

| Variable | Description |
|-----------------|---|
| <delay_int> | The delay, in seconds, between updating the process list. The default is 5 seconds. |
| <max_lines_int> | The maximum number of processes displayed in the output. The default is 20 lines. |

system session list

Command returns a list of all the sessions active on the FortiGate unit. or the current virtual domain if virtual domain mode is enabled.

Syntax

```
get system session list
```

Example output

| PROTO | EXPIRE | SOURCE | SOURCE- | DESTINATION | DESTINATION-NAT |
|-------|--------|--------------------|---------|-------------------|-----------------|
| | NAT | | | | |
| tcp | 0 | 127.0.0.1:1083 | - | 127.0.0.1:514 | - |
| tcp | 0 | 127.0.0.1:1085 | - | 127.0.0.1:514 | - |
| tcp | 10 | 127.0.0.1:1087 | - | 127.0.0.1:514 | - |
| tcp | 20 | 127.0.0.1:1089 | - | 127.0.0.1:514 | - |
| tcp | 30 | 127.0.0.1:1091 | - | 127.0.0.1:514 | - |
| tcp | 40 | 127.0.0.1:1093 | - | 127.0.0.1:514 | - |
| tcp | 60 | 127.0.0.1:1097 | - | 127.0.0.1:514 | - |
| tcp | 70 | 127.0.0.1:1099 | - | 127.0.0.1:514 | - |
| tcp | 80 | 127.0.0.1:1101 | - | 127.0.0.1:514 | - |
| tcp | 90 | 127.0.0.1:1103 | - | 127.0.0.1:514 | - |
| tcp | 100 | 127.0.0.1:1105 | - | 127.0.0.1:514 | - |
| tcp | 110 | 127.0.0.1:1107 | - | 127.0.0.1:514 | - |
| tcp | 103 | 172.20.120.16:3548 | - | 172.20.120.133:22 | - |
| tcp | 3600 | 172.20.120.16:3550 | - | 172.20.120.133:22 | - |
| udp | 175 | 127.0.0.1:1026 | - | 127.0.0.1:53 | - |
| tcp | 5 | 127.0.0.1:1084 | - | 127.0.0.1:514 | - |
| tcp | 5 | 127.0.0.1:1086 | - | 127.0.0.1:514 | - |
| tcp | 15 | 127.0.0.1:1088 | - | 127.0.0.1:514 | - |
| tcp | 25 | 127.0.0.1:1090 | - | 127.0.0.1:514 | - |
| tcp | 45 | 127.0.0.1:1094 | - | 127.0.0.1:514 | - |
| tcp | 59 | 127.0.0.1:1098 | - | 127.0.0.1:514 | - |
| tcp | 69 | 127.0.0.1:1100 | - | 127.0.0.1:514 | - |
| tcp | 79 | 127.0.0.1:1102 | - | 127.0.0.1:514 | - |
| tcp | 99 | 127.0.0.1:1106 | - | 127.0.0.1:514 | - |
| tcp | 109 | 127.0.0.1:1108 | - | 127.0.0.1:514 | - |
| tcp | 119 | 127.0.0.1:1110 | - | 127.0.0.1:514 | - |

| Variable | Description |
|-----------------|--|
| PROTO | The transfer protocol of the session. |
| EXPIRE | How long before this session will terminate. |
| SOURCE | The source IP address and port number. |
| SOURCE-NAT | The source of the NAT. '-' indicates there is no NAT. |
| DESTINATION | The destination IP address and port number. |
| DESTINATION-NAT | The destination of the NAT. '-' indicates there is no NAT. |

system session status

Use this command to display the number of active sessions on the FortiGate unit, or if virtual domain mode is enabled it returns the number of active sessions on the current VDOM. In both situations it will say 'the current VDOM'.

Syntax

```
get system session status
```

Example output

```
The total number of sessions for the current VDOM: 3100
```


system session-helper-info list

Use this command to list the FortiGate session helpers and the protocol and port number configured for each one.

Syntax

```
get system session-helper-info list
```

Example output

```
list builtin help module:
mgcp
dcerpc
rsh
pmap
dns-tcp
dns-udp
rtsp
pptp
sip
mms
tns
h245
h323
ras
tftp
ftp
list session help:
help=pmap, protocol=17 port=111
help=rtsp, protocol=6 port=8554
help=rtsp, protocol=6 port=554
help=pptp, protocol=6 port=1723
help=rtsp, protocol=6 port=7070
help=sip, protocol=17 port=5060
help=pmap, protocol=6 port=111
help=rsh, protocol=6 port=512
help=dns-udp, protocol=17 port=53
help=tftp, protocol=17 port=69
help=tns, protocol=6 port=1521
help=mgcp, protocol=17 port=2727
help=dcerpc, protocol=17 port=135
help=rsh, protocol=6 port=514
help=ras, protocol=17 port=1719
help=ftp, protocol=6 port=21
help=mgcp, protocol=17 port=2427
help=dcerpc, protocol=6 port=135
help=mms, protocol=6 port=1863
help=h323, protocol=6 port=1720
```

system session-info

Use this command to display session information.

Syntax

```
get system session-info expectation
get system session-info full-stat
get system session-info list
get system session-info statistics
get system session-info ttl
```

| Variable | Description |
|-------------|---|
| expectation | Display expectation sessions. |
| full-stat | Display detailed information about the FortiGate session table including a session table and expect session table summary, firewall error statistics, and other information. |
| list | Display detailed information about all current FortiGate sessions. For each session the command displays the protocol number, traffic shaping information, policy information, state information, statistics and other information. |
| statistics | Display the same information as the <code>full-stat</code> command except for the session table and expect session table summary. |
| ttl | Display the current setting of the <code>config system session-ttl</code> command including the overall session timeout as well as the timeouts for specific protocols. |

Example output

```
get system session-info statistics
misc info:                session_count=15 exp_count=0 clash=0
                        memory_tension_drop=0 ephemeral=1/32752 removeable=14
delete=0, flush=0, dev_down=0/0
firewall error stat:
error1=00000000
error2=00000000
error3=00000000
error4=00000000
tt=00000000
cont=00000000
ids_recv=00000000
url_recv=00000000
av_recv=00000000
fqdn_count=00000001
tcp reset stat:
        syncqf=0 acceptqf=0 no-listener=227 data=0 ses=0 ips=0
global: ses_limit=0 ses6_limit=0 rt_limit=0 rt6_limit=0
```

system source-ip

Use this command to list defined source-IPs.

Syntax

```
get system source-ip
```

Example output

```
# get sys source-ip status
```

The following services force their communication to use a specific source IP address:

```
service=NTP source-ip=172.18.19.101
service=DNS source-ip=172.18.19.101
vdom=root service=RADIUS name=server-pc25 source-ip=10.1.100.101
vdom=root service=TACACS+ name=tac_plus_pc25 source-ip=10.1.100.101
vdom=root service=FSAE name=pc26 source-ip=172.18.19.101
vdom=V1 service=RADIUS name=pc25-Radius source-ip=172.16.200.101
vdom=V1 service=TACACS+ name=pc25-tacacs+ source-ip=172.16.200.101
vdom=V1 service=FSAE name=pc16 source-ip=172.16.200.101
```

system startup-error-log

Use this command to display information about system startup errors. This command only displays information if an error occurs when the FortiGate unit starts up.

Syntax

```
get system startup-error-log
```

system status

Use this command to display system status information including:

- FortiGate firmware version, build number and branch point
- virus and attack definitions version
- FortiGate unit serial number and BIOS version
- log hard disk availability
- host name
- operation mode
- virtual domains status: current VDOM, max number of VDOMs, number of NAT and TP mode VDOMs and VDOM status
- current HA status
- system time
- the revision of the WiFi chip in a FortiWiFi unit

Syntax

```
get system status
```

Example output

```
Version: Fortigate-620B v4.0,build0271,100330 (MR2)
Virus-DB: 11.00643(2010-03-31 17:49)
Extended DB: 11.00643(2010-03-31 17:50)
Extreme DB: 0.00000(2003-01-01 00:00)
IPS-DB: 2.00778(2010-03-31 12:55)
FortiClient application signature package: 1.167(2010-04-01 10:11)
Serial-Number: FG600B3908600705
BIOS version: 04000006
Log hard disk: Available
Hostname: 620_ha_1
Operation Mode: NAT
Current virtual domain: root
Max number of virtual domains: 10
Virtual domains status: 1 in NAT mode, 0 in TP mode
Virtual domain configuration: disable
FIPS-CC mode: disable
Current HA mode: a-p, master
Distribution: International
Branch point: 271
Release Version Information: MR2
System time: Thu Apr 1 15:27:29 2010
```

test

Use this command to display information about FortiGate applications and perform operations on FortiGate applications. You can specify an application name and a test level. Enter ? to display the list of applications. The test level performs various functions depending on the application but can include displaying memory usage, dropping connections and restarting the application.

The test levels are different for different applications. In some cases when you enter the command and include an application name but no test level (or an invalid test level) the command output includes a list of valid test levels.

Syntax

```
get test <application_name_str> <test_level_int>
```

Example output

```
get test http
Proxy Worker 0 - http
[0:H] HTTP Proxy Test Usage
[0:H]
[0:H]      2: Drop all connections
[0:H]     22: Drop max idle connections
[0:H]    222: Drop all idle connections
[0:H]      4: Display connection stat
[0:H]     44: Display info per connection
[0:H]    444: Display connections per state
[0:H]   4444: Display per-VDOM statistics
[0:H]  44444: Display information about idle connections
[0:H]    55: Display tcp info per connection

get test http 4
HTTP Common
Current Connections                                0/8032

HTTP Stat
Bytes sent                                          0 (kb)
Bytes received                                     0 (kb)
Error Count (alloc)                               0
Error Count (accept)                              0
Error Count (bind)                                0
Error Count (connect)                             0
Error Count (socket)                              0
Error Count (read)                                0
Error Count (write)                                0
Error Count (retry)                               0
Error Count (poll)                                0
Error Count (scan reset)                          0
Error Count (urlfilter wait)                      0
```

| | |
|-------------------------------------|---|
| Last Error | 0 |
| Web responses clean | 0 |
| Web responses scan errors | 0 |
| Web responses detected | 0 |
| Web responses infected with worms | 0 |
| Web responses infected with viruses | 0 |
| Web responses infected with susp | 0 |
| Web responses file blocked | 0 |
| Web responses file exempt | 0 |
| Web responses bannedword detected | 0 |
| Web requests oversize pass | 0 |
| Web requests oversize block | 0 |
| URL requests exempt | 0 |
| URL requests blocked | 0 |
| URL requests passed | 0 |
| URL requests submit error | 0 |
| URL requests rating error | 0 |
| URL requests rating block | 0 |
| URL requests rating allow | 0 |
| URL requests infected with worms | 0 |
| Web requests detected | 0 |
| Web requests file blocked | 0 |
| Web requests file exempt | 0 |
| POST requests clean | 0 |
| POST requests scan errors | 0 |
| POST requests infected with viruses | 0 |
| POST requests infected with susp | 0 |
| POST requests file blocked | 0 |
| POST requests bannedword detected | 0 |
| POST requests oversize pass | 0 |
| POST requests oversize block | 0 |
| Web request backlog drop | 0 |
| Web response backlog drop | 0 |

HTTP Accounting

setup_ok=0 setup_fail=0 conn_ok=0 conn_inp=0
urlfilter=0/0/0 uf_lookupf=0
scan=0 clt=0 srv=0

user adgrp

Use this command to list Directory Service user groups.

Syntax

```
get user adgrp [<dsgroupname>]
```

If you do not specify a group name, the command returns information for all Directory Service groups. For example:

```
== [ DOCTEST/Cert Publishers ]
name: DOCTEST/Cert Publishers      server-name: DSserv1
== [ DOCTEST/Developers ]
name: DOCTEST/Developers          server-name: DSserv1
== [ DOCTEST/Domain Admins ]
name: DOCTEST/Domain Admins       server-name: DSserv1
== [ DOCTEST/Domain Computers ]
name: DOCTEST/Domain Computers    server-name: DSserv1
== [ DOCTEST/Domain Controllers ]
name: DOCTEST/Domain Controllers  server-name: DSserv1
== [ DOCTEST/Domain Guests ]
name: DOCTEST/Domain Guests       server-name: DSserv1
== [ DOCTEST/Domain Users ]
name: DOCTEST/Domain Users        server-name: DSserv1
== [ DOCTEST/Enterprise Admins ]
name: DOCTEST/Enterprise Admins   server-name: DSserv1
== [ DOCTEST/Group Policy Creator Owners ]
name: DOCTEST/Group Policy Creator Owners  server-name: DSserv1
== [ DOCTEST/Schema Admins ]
name: DOCTEST/Schema Admins       server-name: DSserv1
```

If you specify a Directory Service group name, the command returns information for only that group. For example:

```
name           : DOCTEST/Developers
server-name    : ADServ1
```

The `server-name` is the name you assigned to the Directory Service server when you configured it in the `user fsae` command.

vpn ike gateway

Use this command to display information about FortiGate IPsec VPN IKE gateways.

Syntax

```
get vpn ike gateway [<gateway_name_str>]
```

vpn ipsec tunnel details

Use this command to display information about IPsec tunnels.

Syntax

```
get vpn ipsec tunnel details
```

vpn ipsec tunnel name

Use this command to display information about a specified IPsec VPN tunnel.

Syntax

```
get vpn ipsec tunnel name <tunnel_name_str>
```

vpn ipsec stats crypto

Use this command to display information about the FortiGate hardware and software crypto configuration.

Syntax

```
get vpn ipsec stats crypto
```

Example output

```
get vpn ipsec stats crypto
```

IPsec crypto devices in use:

CP6 (encrypted/decrypted):

| | | |
|-------|---|---|
| null: | 0 | 0 |
| des: | 0 | 0 |
| 3des: | 0 | 0 |
| aes: | 0 | 0 |

CP6 (generated/validated):

| | | |
|---------|---|---|
| null: | 0 | 0 |
| md5: | 0 | 0 |
| sha1: | 0 | 0 |
| sha256: | 0 | 0 |

SOFTWARE (encrypted/decrypted):

| | | |
|-------|---|---|
| null: | 0 | 0 |
| des: | 0 | 0 |
| 3des: | 0 | 0 |
| aes: | 0 | 0 |

SOFTWARE (generated/validated):

| | | |
|---------|---|---|
| null: | 0 | 0 |
| md5: | 0 | 0 |
| sha1: | 0 | 0 |
| sha256: | 0 | 0 |

vpn ipsec stats tunnel

Use this command to view information about IPsec tunnels.

Syntax

```
get vpn ipsec stats tunnel
```

Example output

```
#get vpn ipsec stats tunnel
tunnels
  total: 0
  static/ddns: 0
  dynamic: 0
  manual: 0
  errors: 0
selectors
  total: 0
  up: 0
```

vpn ssl monitor

Use this command to display information about logged in SSL VPN users and current SSL VPN sessions.

Syntax

```
get vpn ssl monitor
```

Example output

```
FortiGate 300 # get vpn ssl monitor
```

```
SSL-VPN Login Users:
```

| Index | User | Auth Type | Timeout | From | HTTP in/out | HTTPS in/out |
|-------|------|-----------|---------|------|-------------|--------------|
|-------|------|-----------|---------|------|-------------|--------------|

```
SSL-VPN sessions:
```

| Index | User | Source IP | Tunnel/Dest IP |
|-------|------|-----------|----------------|
|-------|------|-----------|----------------|

vpn status l2tp

Use this command to display information about L2TP tunnels.

Syntax

```
get vpn status l2tp
```

vpn status pptp

Use this command to display information about PPTP tunnels.

Syntax

```
get vpn status pptp
```


vpn status ssl

Use this command to display SSL VPN tunnels and to also verify that the FortiGate unit includes the CP6 or greater FortiASIC device that supports SSL acceleration.

Syntax

```
get vpn status ssl hw-acceleration-status  
get vpn status ssl list
```

| Variable | Description |
|------------------------|---|
| hw-acceleration-status | Display whether or not the FortiGate unit contains a FortiASIC device that supports SSL acceleration. |
| list | Display information about all configured SSL VPN tunnels. |

webfilter ftgd-statistics

Use this command to display FortiGuard Web Filtering rating cache and daemon statistics.

Syntax

```
get webfilter ftgd-statistics
```

Example output

```
get webfilter ftgd-statistics
```

Rating Statistics:

=====

| | | |
|--------------------------------|---|---|
| DNS failures | : | 0 |
| DNS lookups | : | 0 |
| Data send failures | : | 0 |
| Data read failures | : | 0 |
| Wrong package type | : | 0 |
| Hash table miss | : | 0 |
| Unknown server | : | 0 |
| Incorrect CRC | : | 0 |
| Proxy request failures | : | 0 |
| Request timeout | : | 0 |
| Total requests | : | 0 |
| Requests to FortiGuard servers | : | 0 |
| Server errored responses | : | 0 |
| Relayed rating | : | 0 |
| Invalid profile | : | 0 |
| | | |
| Allowed | : | 0 |
| Blocked | : | 0 |
| Logged | : | 0 |
| Errors | : | 0 |

Cache Statistics:

=====

| | | |
|----------------|---|---|
| Maximum memory | : | 0 |
| Memory usage | : | 0 |
| | | |
| Nodes | : | 0 |
| Leaves | : | 0 |
| Prefix nodes | : | 0 |
| Exact nodes | : | 0 |
| | | |
| Requests | : | 0 |
| Misses | : | 0 |
| Hits | : | 0 |
| Prefix hits | : | 0 |
| Exact hits | : | 0 |

| | | |
|---------------------|---|----|
| No cache directives | : | 0 |
| Add after prefix | : | 0 |
| Invalid DB put | : | 0 |
| DB updates | : | 0 |
| | | |
| Percent full | : | 0% |
| Branches | : | 0% |
| Leaves | : | 0% |
| Prefix nodes | : | 0% |
| Exact nodes | : | 0% |
| | | |
| Miss rate | : | 0% |
| Hit rate | : | 0% |
| Prefix hits | : | 0% |
| Exact hits | : | 0% |

webfilter status

Use this command to display FortiGate Web Filtering rating information.

Syntax

```
get webfilter status [<refresh-rate_int>]
```

wireless-controller rf-analysis

Use this command to show information about RF conditions at the access point.

Syntax

```
get wireless-controller rf-analysis [<wtp_id>]
```

Example output

```
# get wireless-controller rf-analysis
```

```
<wtp-id>      wtp id
```

```
FWF60C3G11004319 (global) # get wireless-controller rf-analysis
```

```
WTP: FWF60C-WIFI0 0-127.0.0.1:15246
```

| channel | rssi-total | rf-score | overlap-ap | interfere-ap |
|---------|------------|----------|------------|--------------|
| 1 | 418 | 1 | 24 | 26 |
| 2 | 109 | 5 | 0 | 34 |
| 3 | 85 | 7 | 1 | 34 |
| 4 | 64 | 9 | 0 | 35 |
| 5 | 101 | 6 | 1 | 35 |
| 6 | 307 | 1 | 8 | 11 |
| 7 | 82 | 7 | 0 | 16 |
| 8 | 69 | 8 | 1 | 15 |
| 9 | 42 | 10 | 0 | 15 |
| 10 | 53 | 10 | 0 | 14 |
| 11 | 182 | 1 | 5 | 6 |
| 12 | 43 | 10 | 0 | 6 |
| 13 | 20 | 10 | 0 | 5 |
| 14 | 8 | 10 | 0 | 5 |

```
Controller: FWF60C3G11004319-0
```

| channel | rssi_total |
|---------|------------|
| 1 | 418 |
| 2 | 109 |
| 3 | 85 |
| 4 | 64 |
| 5 | 101 |
| 6 | 307 |
| 7 | 82 |
| 8 | 69 |
| 9 | 42 |
| 10 | 53 |
| 11 | 182 |
| 12 | 43 |
| 13 | 20 |
| 14 | 8 |

wireless-controller scan

Use this command to view the list of access points detected by wireless scanning.

Syntax

```
get wireless-controller scan
```

Example output

| CMW | SSID | BSSID | CHAN | RATE | S:N | INT | CAPS | ACT | LIVE | AGE |
|-----|----------|-------------------|------|------|------|-----|------|-----|-------|------|
| | WIRED | | | | | | | | | |
| UNN | | 00:0e:8f:24:18:6d | 64 | 54M | 16:0 | 100 | Es | N | 62576 | 1668 |
| | ? | | | | | | | | | |
| UNN | ftiguest | 00:15:55:23:d8:62 | 157 | 130M | 6:0 | 100 | EPs | N | 98570 | 2554 |
| | ? | | | | | | | | | |

wireless-controller status

Use this command to view the numbers of wtp sessions and clients.

Syntax

```
get wireless-controller status
```

Example output

```
# get wireless-controller status
Wireless Controller :
    wtp-session-count: 1
    client-count      : 1/0
```

wireless-controller vap-status

Use this command to view information about your SSIDs.

Syntax

```
get wireless-controller vap-status
```

Example output

```
# get wireless-controller vap-status
WLAN: mesh.root
      name           : mesh.root
      vdom            : root
      ssid            : fortinet.mesh.root
      status          : up
      mesh backhaul   : yes
      ip              : 0.0.0.0
      mac             : 00:ff:0a:57:95:ca
      station info    : 0/0
WLAN: wifi
      name           : wifi
      vdom            : root
      ssid            : ft-mesh
      status          : up
      mesh backhaul   : yes
      ip              : 10.10.80.1
      mac             : 00:ff:45:e1:55:81
      station info    : 1/0
```


wireless-controller wlchanlistlic

Use this command to display a list of the channels allowed in your region, including

- the maximum permitted power for each channel
- the channels permitted for each wireless type (802.11n, for example)

The list is in XML format.

Syntax

```
get wireless-controller wlchanlistlic
```

Sample output

```
country name: UNITED STATES2, country code:841, iso name:US
channels on 802.11A band without channel bonding:
channel= 36  maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 40  maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 44  maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 48  maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel=149  maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=153  maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=157  maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=161  maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=165  maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2

channels on 802.11B band without channel bonding:
channel=  1  maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel=  2  maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel=  3  maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel=  4  maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel=  5  maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel=  6  maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel=  7  maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel=  8  maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel=  9  maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 10  maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 11  maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2

channels on 802.11G band without channel bonding:
channel=  1  maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel=  2  maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel=  3  maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel=  4  maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel=  5  maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel=  6  maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel=  7  maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel=  8  maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel=  9  maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
```

```
channel= 10 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 11 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
```

channels on 802.11N 2.4GHz band without channel bonding:

```
channel= 1 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 2 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 3 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 4 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 5 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 6 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 7 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 8 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 9 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 10 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 11 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
```

channels on 802.11N 2.4GHz band with channel bonding plus:

```
channel= 1 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 2 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 3 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 4 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 5 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 6 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 7 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
```

channels on 802.11N 2.4GHz band with channel bonding minus:

```
channel= 5 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 6 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 7 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 8 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 9 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 10 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
channel= 11 maxRegTxPower= 27 maxTxPower= 63/2 minTxPower= 63/2
```

channels on 802.11N 5GHz band without channel bonding:

```
channel= 36 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 40 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 44 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 48 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel=149 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=153 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=157 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=161 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
channel=165 maxRegTxPower= 30 maxTxPower= 63/2 minTxPower= 63/2
```

channels on 802.11N 5GHz band with channel bonding all:

```
channel= 36 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 40 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
channel= 44 maxRegTxPower= 23 maxTxPower= 63/2 minTxPower= 63/2
```

```
channel= 48  maxRegTxPower= 23  maxTxPower= 63/2  minTxPower= 63/2
channel=149  maxRegTxPower= 30  maxTxPower= 63/2  minTxPower= 63/2
channel=153  maxRegTxPower= 30  maxTxPower= 63/2  minTxPower= 63/2
channel=157  maxRegTxPower= 30  maxTxPower= 63/2  minTxPower= 63/2
channel=161  maxRegTxPower= 30  maxTxPower= 63/2  minTxPower= 63/2
```

wireless-controller wtp-status

Syntax

```
get wireless-controller wtp-status
```

Example output

```
# get wireless-controller wtp-status
WTP: FAP22B3U11005354 0-192.168.3.110:5246
  wtp-id           : FAP22B3U11005354
  region-code      :
  name             :
  mesh-uplink      : mesh
  mesh-downlink    : disabled
  mesh-hop-count   : 1
  parent-wtp-id    :
  software-version :
  local-ipv4-addr  : 0.0.0.0
  board-mac        : 00:00:00:00:00:00
  join-time        : Mon Apr  2 10:23:32 2012
  connection-state : Disconnected
  image-download-progress: 0
  last-failure     : 0 -- N/A
  last-failure-param:
  last-failure-time: N/A
Radio 1           : Monitor
Radio 2           : Ap
  country-name     : NA
  country-code     : N/A
  client-count     : 0
  base-bssid       : 00:00:00:00:00:00
  max-vaps         : 7
  oper-chan        : 0
Radio 3           : Not Exist
WTP: FWF60C-WIFI0 0-127.0.0.1:15246
  wtp-id           : FWF60C-WIFI0
  region-code      : ALL
  name             :
  mesh-uplink      : ethernet
  mesh-downlink    : enabled
  mesh-hop-count   : 0
  parent-wtp-id    :
  software-version : FWF60C-v5.0-build041
  local-ipv4-addr  : 127.0.0.1
  board-mac        : 00:09:0f:fe:cc:56
  join-time        : Mon Apr  2 10:23:35 2012
  connection-state : Connected
  image-download-progress: 0
  last-failure     : 0 -- N/A
```

```
last-failure-param:
last-failure-time: N/A
Radio 1           : Ap
country-name      : US
country-code      : N/A
client-count      : 1
base-bssid        : 00:0e:8e:3b:63:99
max-vaps          : 7
oper-chan         : 1
Radio 2           : Not Exist
Radio 3           : Not Exist
```

tree

The `tree` command displays FortiOS `config` CLI commands in a tree structure called the configuration tree. Each configuration command forms a branch of the tree.

Syntax

```
tree [branch] [sub-branch]
```

You can enter the `tree` command from the top of the configuration tree the command displays the complete configuration tree. Commands are displayed in the order that they are processed when the FortiGate unit starts up. For example, the following output shows the first 10 lines of `tree` command output:

```
tree
-- -- system -- [vdom] --*name (12)
      +- vcluster-id (0,0)
      |- <global> -- language
            |- gui-ipv6
            |- gui-voip-profile
            |- gui-lines-per-page (20,1000)
            |- admintimeout (0,0)
            |- admin-concurrent
            |- admin-lockout-threshold (0,0)
            |- admin-lockout-duration (1,2147483647)
            |- refresh (0,2147483647)
            |- interval (0,0)
            |- failtime (0,0)
            |- daily-restart
            |- restart-time
      ...
```

You can include a branch name with the `tree` command to view the commands in that branch:

```
tree user
-- user -- [radius] --*name (36)
      |- server (64)
      |- secret
      |- secondary-server (64)
      |- secondary-secret
      ...
      |- [tacacs+] --*name (36)
            |- server (64)
            |- secondary-server (64)
            |- tertiary-server (64)
            ...
      |- [ldap] --*name (36)
            |- server (64)
            |- secondary-server (64)
            |- tertiary-server (64)
            |- port (1,65535)
      ...
```

You can include a branch and sub branch name with the `tree` command to view the commands in that sub branch:

```
tree user local
-- [local] --*name (36)
    |- status
    |- type
    |- passwd
    |- ldap-server (36)
    |- radius-server (36)
    +- tacacs+-server (36)
    ...
```

If you enter the `tree` command from inside the configuration tree the command displays the tree for the current command:

```
config user ldap
tree
-- [ldap] --*name (36)
    |- server (64)
    |- cnid (21)
    |- dn (512)
    |- port (1,65535)
    |- type
    ...
```

The `tree` command output includes information about field limits. These apply in both the CLI and the web-based manager. For a numeric field, the two numbers in parentheses show the lower and upper limits. For example (0,32) indicates that values from 0 to 32 inclusive are accepted. For string values, the number in parentheses is one more than the maximum number of characters permitted.

In the following example, the FQDN can contain up to 255 characters.

```
config firewall address
tree
-- [address] --*name (64)
    |- subnet
    |- type
    |- start-ip
    |- end-ip
    |- fqdn (256)
    |- country (3)
    |- cache-ttl (0,86400)
    |- wildcard
    |- comment
    |- visibility
    |- associated-interface (36)
    |- color (0,32)
    +- [tags] --*name (64)
```